Lab LL01
Domino and WebSphere Integration on iSeries Server

ITSO iSeries Technical Forum 2001

Presented by
Wilfried Blankertz
Debbie Landon
Wendy Thomson
Xiao Song Zhu

Contents

Part 1. Overview 1

Overview of the lab 3
Lab parameters table 4
Classroom environment 4

Part 2. Main lab 7

Lab 1. Developing a Domino application 9
Objectives 9
Task 1: Completing the design of a Web application using Domino Designer . . . 9
Task 2: Configuring the Domino HTTP task 11
Task 3: Testing a Domino application from a Web browser 14

Lab 2. Creating a simple Web application 17
Objectives 17
Task 1: Creating an instance of the WebSphere Application Server 17
Task 2: Configuring Domino for AS/400 as an HTTP server for WebSphere . . 18
Task 3: Modifying and compiling a simple Java servlet on the iSeries server . . 24
Task 4: Creating a Web application 30
Task 5: Testing SimpleServlet 41

Lab 3. Enabling Domino authentication 43
Objectives 43
Task 1: Securing your Domino database 43
Task 2: Experiencing the Domino security challenge 43

Lab 4. Enabling WebSphere authentication 47
Objectives 47
Task 1: Configuring Domino as an LDAP server 47
Task 2: Enabling security for the WebSphere Application Server 3.5.2 50
Task 3: Protecting WebSphere components of the sample Web application . . . 59
Task 4: Verifying WebSphere security 71

Lab 5. Configuring Single Sign-On for WebSphere and Domino 73
Objectives 73
Task 1: Configuring WebSphere for Single Sign-On 73
Task 2: Creating the Domino Web Single Sign-On configuration document . . . 77
Task 3: Configuring the Domino Server document for Single Sign-On 81
Task 4: Verifying Single Sign-On between WebSphere and Domino 83

Part 3. Appendices 89

Lab 6. Optional lab: Using the OS/400 LDAP server 91
Objectives 91
Task 1: Checking your connection to OS/400 LDAP 91
Task 2: Changing WebSphere to use OS/400 LDAP 92
Task 3: Creating a Directory Assistance Domino database 97
Task 4: Changing the Domino Server to use OS/400 LDAP 100
Task 5: Verifying Single Sign-On between Domino and WebSphere 106

Lab 7. Optional lab: Using IBM HTTP Server for OS/400 113
Objectives 113
Task 1: Changing the HTTP configuration on your Domino Server 113
Task 2: Creating an instance of the IBM HTTP Server for OS/400 114
Task 3: Testing your OS/400 HTTP configuration 118
Task 4: Reconfiguring the OS/400 HTTP Server for Domino 119
Task 5: Verifying Single Sign-On between Domino and WebSphere 122

Lab 8. Information only: Configuring the OS/400 LDAP server 129
Objectives 129
Task 1: Pre-configuration tasks for OS/400 LDAP 129
Task 2: Configuring OS/400 LDAP 130
Task 3: Starting the OS/400 LDAP server 133
Task 4: Publishing to LDAP from the OS/400 System Distribution Directory . 134
Task 5: Verifying the connection to OS/400 LDAP 136

Part 1. Overview

Read this section *before* starting the lab. This section contains information on the class environment and on how the labs are set up and organized. It also contains a table that shows the different values and parameters you need to know. The values and parameters are specific and unique to each team in the lab.

Overview of the lab

These lab exercises use a very simple example to access a Domino for AS/400 application and a Java servlet running in a WebSphere Application Server on the same iSeries 400 or AS/400 server. This simple example shows how to configure security on Domino and WebSphere and how to enable the Single Sign-On capabilities of both products.

This workshop includes the following lab exercises:

- In Lab 1. “Developing a Domino application” on page 9, you update a Domino application by creating a database on a Domino for AS/400 R5.0.6a server, which can be accessed from a Web Browser.
- In Lab 2. “Creating a simple Web application” on page 17, you update a simple Java servlet and place it into an instance of a WebSphere Application Server 3.5.2 for the iSeries server.
- In Lab 3. “Enabling Domino authentication” on page 43, you configure the Domino application so that a Web Browser can only open the database after supplying a valid user name and password (which must exist in the Domino Directory).
- In Lab 4. “Enabling WebSphere authentication” on page 47, you configure WebSphere Application Server 3.5.2 security so that a user can only start a Web application after supplying a valid user name and password. The user name and password must exist in the Domino Directory (accessed through LDAP).
- In Lab 5. “Configuring Single Sign-On for WebSphere and Domino” on page 73, you learn how to configure WebSphere and Domino to avoid requiring users to key in the their user name and password a second time when a Domino application links them to a WebSphere resource, or when a WebSphere resource links them to a Domino application.
- In Lab 6. “Optional lab: Using the OS/400 LDAP server” on page 91, you learn how to use SecureWay Directory for OS/400 as the user registry instead of the Domino directory that is used in the previous exercises.
- In Lab 7. “Optional lab: Using IBM HTTP Server for OS/400” on page 113, you use OS/400 HTTP server, instead of the Lotus Domino for AS/400 HTTP server that is used in the previous exercises. You also configure the Domino Plug-in for OS/400 HTTP Server to allow you to use the OS/400 HTTP server, instead of the Domino HTTP server, to serve Domino applications as well.
- Lab 8. “Information only: Configuring the OS/400 LDAP server” on page 129, is included for informational purposes only. It contains the steps required for configuring OS/400 LDAP and publishing the System Distribution Directory (SDD) to the LDAP directory. Because these functions can only be done once on an iSeries server, they are not practical in a lab environment where multiple teams are running on one system.

Lab parameters table

Several parameters should be correctly entered throughout this lab. Table 1 shows the values that should be used to successfully complete the lab. Make sure you always replace *xx* with your team number.

Note: If you choose the wrong value for xx, you and other students will have problems successfully finishing the exercises.

Table 1. Lab table with parameters used for the classroom

Environment	Value	Descriptions
Team #	**xx**	Team number - refer to your workstation tent card
AS/400	PWDI	iSeries 400 or AS/400 server system name
	DOMWASxx	OS/400 user profile (*xx* = team number)
	dom2was	OS/400 user profile password
	PID.IBM.COM	OS/400 TCP/IP Domain Name
Domino	DOMWASxx	Domino Server (*xx* = team number)
	Domxx	Domino Organization (*xx* = team number)
	/DomWasLab/xx	Domino Data Directory (*xx* = team number)
	Notes Guru	Domino Administrator (First Name Last Name)
	dom2was	Domino Administrator password (& internet password)
	nguru	Domino Administrator Short name
	DomWASLab.nsf	Domino Lab Database
	80xx	Domino HTTP Port (default 80, *xx* = team number)
	389xx	Port used for Domino LDAP Server
OS/400 LDAP	ou=ITSO,o=IBM,c=US	OS/400 LDAP Distinguished Name
	cn = Administrator	OS/400 LDAP Administrator
	ldappw	OS/400 LDAP Administrator password
WebSphere Application Server (WAS)	WASxx	WAS Instance name (*xx*=team number)
	9xx	WAS Administrator Port (default 900, *xx*=team)
	80xx	WAS HTTP Port (default 80, *xx*=team)
	90xx	WAS LSD Port (default 9000, *xx*=team)
	SimpleServlet	Servlet Name

Classroom environment

Because there are multiple students in the class, some necessary resources are not available to all the students. Therefore, the lab setup is somewhat different from what would be done in a real world environment. This section illustrates when students have to share a resource. It also explains when unusual configuration parameters are used to allow multiple resources on a single iSeries 400 or AS/400 server.

All student teams *share* the same*:*

- TCP/IP network
- iSeries 400 or AS/400 server, although there may be more than one system for the entire class
- The SecureWay Directory for OS/400 LDAP server (it will be already configured for this lab)

Each student team has an *individual*:

- Partitioned Domino for AS/400 R5.06a server
- Instance of the OS/400 HTTP server
- Instance of the WebSphere Application Server 3.5.2
- WebSphere Administration Console
- Lotus Notes clients

Because of the environment explained above, the following setup parameters are different from a real world environment (*xx* denotes the team number):

- Because there is a separate Domino server for each student team, a unique IP address in the form 9.5.33.1yy (where yy is your team **number + 40**) is assigned to each team (on port 1352) to connect to the Notes clients. The names of the Domino servers are `DomWASxx`. Each Domino server needs to be in a different Domain and Organization, both called `Domxx`.
- To allow each student team to configure a WebSphere Application Server 3.5.2, a separate instance with the name `WASxx` is set up for each team.
- By default, the WebSphere Administrative Console communicates with the WebSphere Administrative Server via port 900. To allow multiple instances on the same iSeries 400 or AS/400 server, the port should be set to `9xx`.

  Note: The 900 range and the 9000 range are different things.
- By default, the Location Service Daemon (LSD), as part of the WebSphere Administrative Server, listens to port 9000 to communicate with the WebSphere Application Server 3.5.2. To allow multiple instances on the same AS/400 system, the port should be set to `90xx`.

  Note: The 900 range and 9000 range are different things.
- HTTP servers usually listen to port 80 to allow Web Browsers to connect. Again, to allow multiple servers on the same system, set the port numbers to `80xx`.

Good luck, and enjoy completing these labs!

Part 2. Main lab

Lab 1. Developing a Domino application

The purpose of this exercise is use Domino Designer to update a simple Domino Web application. This application is used later in the lab to test user authentication and Single Sign-On when combined with a servlet running on a WebSphere Application Server.

Objectives

This lab teaches you how to:

- Complete the design of a Domino Web application.
- Configure the Domino HTTP server to listen on a specific TCP/IP port.
- Access the Domino Web Application from a Web browser to verify your setup.

Important

Throughout these lab exercises, replace *xx* with your team number. Also, refer to Table 1 on page 4 to ensure that the correct values for the configuration parameters are entered.

Task 1: Completing the design of a Web application using Domino Designer

This objective of this task is to update an existing Domino Web application using Domino Designer. This Web application is used in later labs to test user authentication and Single Sign-On when accessing this application with a browser and linking to a servlet running on a WebSphere Application Server.

Follow this process to add the Domino Web application to your workspace and open it for editing:

__ 1. Check the Windows task bar, whether the Domino Designer has already been started and click the icon. If it has not been started yet, do so by selecting:

Start->Programs->Lotus Applications->Domino Designer

__ 2. You are prompted for the password for the Lotus Notes user (Notes Guru/Domxx). Enter the password `dom2was`. Click **OK**.

__ 3. From the Domino Designer window, open the Domino Web application by selecting the pull-down menu options **File->Database->Open** (or use the shortcut Ctl-O).

__ 4. In the Server field of the Open Database window, specify your Domino server name (DomWASxx). Remember to replace *xx* with your team number.

__ 5. In the Filename field of the Open Database window, enter DomWASLab.nsf (or select the **Domino WebSphere Lab** database), and click **Open** (see Figure 1 on page 10).

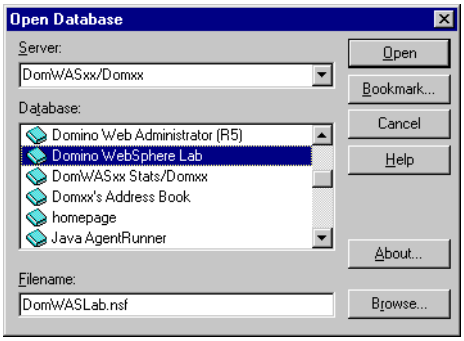

Figure 1. Opening the Domino Web application (DomWASLab.nsf) database

__ 6. Click the **Forms** view and open the **LoanApp** form for editing (Figure 2). You may receive a warning at this point that the signer of the database is not known in your address book. If so, click Yes.

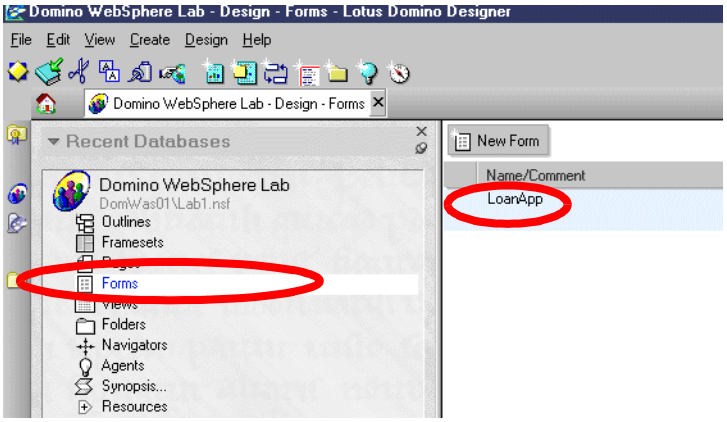

Figure 2. Domino Designer: Forms view - LoanApp form

Include a link to a servlet running under WebSphere

Follow these steps to include a link to a servlet running under WebSphere.

Note

Later in this lab, user authentication and Single Sign-On is demonstrated by linking between both WebSphere and Domino application servers. The *$$Return* field in the LoanApp form is used to link the user to the WebSphere application.

__ 1. Scroll down the LoanApp form and click on the **$$Return** field to change the *Default Value* of that field (Figure 3).

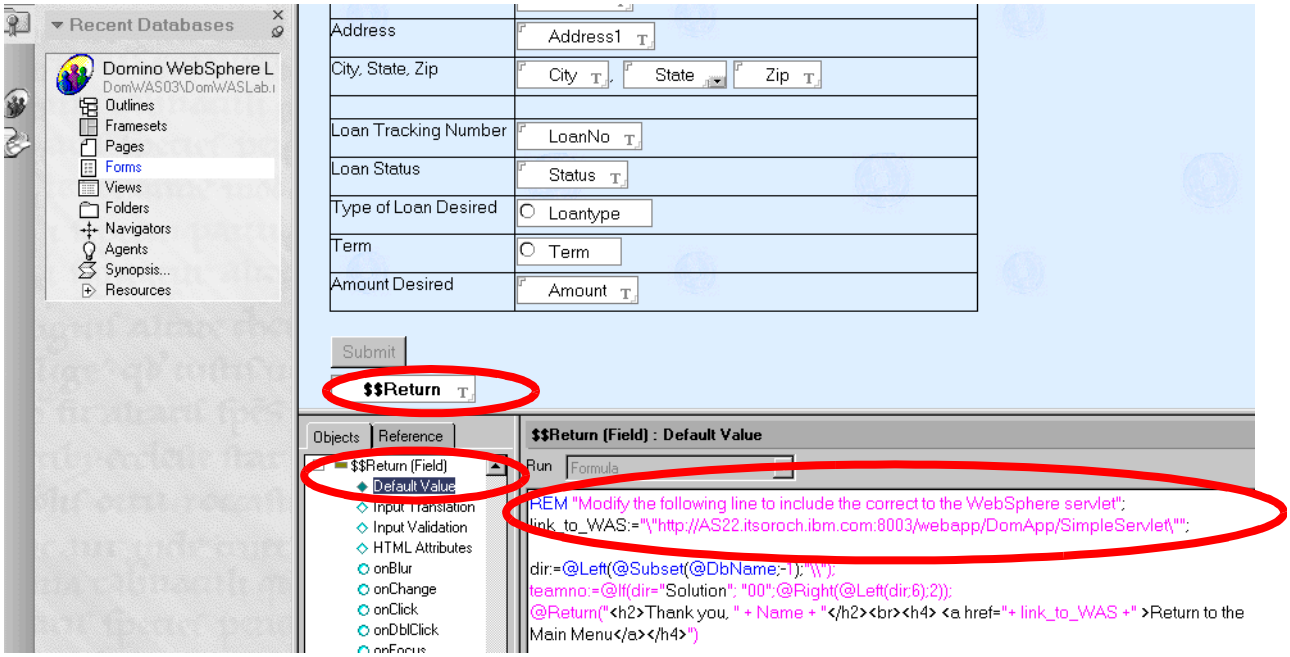

Figure 3. $$Return Field: Changing the value

__ 2. Change the value assigned to the link_to_WAS variable shown in Figure 3 to:

```
"\"http://PWDI.PID.IBM.COM:80xx/webapp/DomApp/SimpleServlet\""
```

Make sure you include the `"\"` at the beginning and the `\""` at the end of the string. The backslash (\) must be there because the inner double quotes (") need to be part of the string.

This Web path is defined later in this lab. Make sure you replace the *xx* with your team number. The AS22 value in Figure 3 refers to the host name of your iSeries 400 or AS/400 server used for this lab . This value should be replaced to the one shown in your lab parameters table (PWDI in Table 1 on page 4).

__ 3. Click the green check mark ( ) to save the Default Value formula.

__ 4. Save and close the Form Design window (the fastest way is to press Ctrl+s and than press Esc).

__ 5. Close the Domino Designer window.

Task 2: Configuring the Domino HTTP task

For this lab, where multiple students are using their Domino HTTP server on the same iSeries 400 or AS/400 server, some configuration steps are needed to ensure that each HTTP server uses a different port or a unique IP address.

By default, the HTTP servers of both products listen to port 80 on all IP addresses defined to any of the communication adapters on the iSeries 400 or AS/400 server. This creates a conflict if you start both HTTP servers at the same time. For the purposes of this lab, define unique ports for each student team (80xx, where *xx* is the team number).

WebSphere Application Server 3.5.2 relies on an HTTP server, which can be either IBM HTTP Server for OS/400 or Lotus Domino for AS/400 (V 5.04 or higher. However, for Single Sign-On capability V 5.0.6a is needed). The first part of this lab uses the Lotus Domino for AS/400 server HTTP task. Later, in Lab 7. “Optional lab: Using IBM HTTP Server for OS/400” on page 113, you have the option to change the configuration to use the IBM HTTP Server for OS/400 instead.

Perform the following steps to configure Domino to use port 80xx for HTTP:

__ 1. Check the Windows task bar, whether the Domino Administrator has already been started and click the icon. If it has not been started yet, do so by selecting:

Start->Programs->Lotus Applications->Domino Administrator

__ 2. You are prompted for the password for Notes Guru/Domxx. Enter the password `dom2was`. Click **OK**.

__ 3. Click the **Configuration** tab and expand the **Server** folder. Open the **All Servers Documents** view.

__ 4. Click on the Domino Server document (DOMWASxx) for your Domino server, and click the **Edit Server** button.

__ 5. Click the **Ports** tab, and then click the **Internet Ports** tab. Then, click the **Web** tab. Change the TCP/IP port number field to `80xx`, where *xx* is your team number. The results are shown in Figure 4.

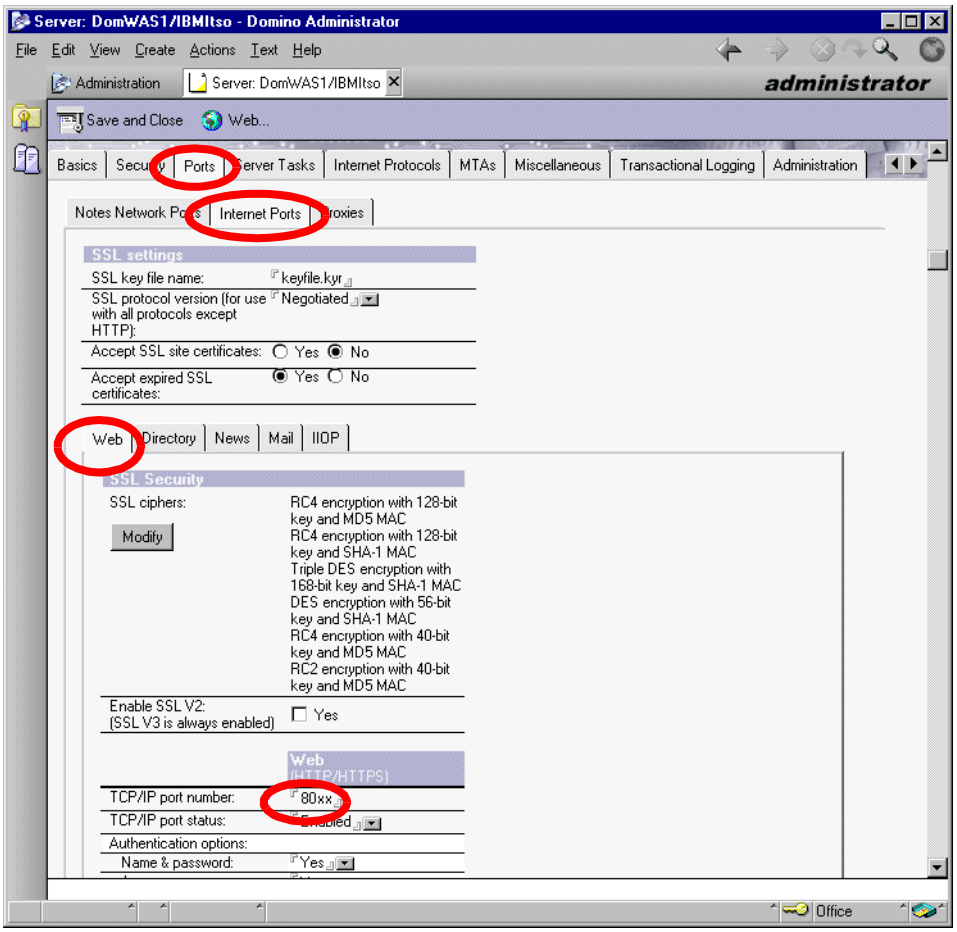

Figure 4. Changing the HTTP port number for Domino

__ 6. Click the **Save and Close** button to exit the Domino Server document.

Starting the HTTP task of your Lotus Domino for AS/400 server

Follow these steps to start the HTTP task of your Lotus Domino for AS/400 server:

__ 1. On your Windows Task Bar, check if the 5250 emulation has already been started, otherwise double-click the icon for the 5250 emulation session for your lab system (PWDI).

__ 2. Sign on to the lab iSeries 400 or AS/400 server PWDI (user ID `DOMWASxx` and password `dom2was`).

__ 3. Enter the following command on the OS/400 command line and press Enter:

```
WRKDOMSVR DOMWASxx
```

__ 4. Enter option `8` (Work console) into the Opt field next to *your* Domino server (DOMWASxx) and press Enter.

__ 5. From the Domino console, enter the following Domino command on the command line and press Enter:

```
load http
```

This starts the Domino HTTP server task.

__ 6. Press F5 to update the console display. Receiving the messages similar to those shown in Figure 5 verifies a successful start. It may take a minute until you see the final message.

```
                          Work with Domino Console
                                                  Server: DOMWASxx
Previous subcommands and messages:



> load http

  > load http


  03/01/2001 05:19:00 PM  JVM: Java Virtual Machine initialized.
  03/01/2001 05:19:00 PM  Creating Domino Web Administrator database...
  03/01/2001 05:19:24 PM  Domino Web Administrator database created
  03/01/2001 05:19:27 PM  HTTP Web Server started
Enter a Domino subcommand.
===>

F3=Exit    F5=Refresh    F6=Print    F9=Retrieve
F17=Top    F18=Bottom    F21=Command line
```

Figure 5. Load HTTP Domino command

__ 7. Use the the `show tasks` Domino console command, to verify the HTTP tasks is actually listening to port 80xx, by entering the following command:

```
sh ta
```

__ 8. Press F5 to update the console display. You may have to press page forward to see the status of the HTTP task.

__ 9. Press function key F3 to exit the Domino console and minimize the 5250 emulation window.

Task 3: Testing a Domino application from a Web browser

Perform the following steps to verify that you can successfully access the Domino application from a Web browser before continuing with the next lab. At this point, no security has been enabled.

__ 1. Start your Netscape Web browser.

__ 2. You must change your Netscape Web browser to accept cookies before testing. From the Netscape window, select the **Edit->Preferences** pull-down menu options.

__ 3. Click **Advanced** in the left column of the Preferences window.

__ 4. In the Cookies box on the right side of the screen, ensure that Accept all Cookies radio button is selected and that the Warn me before accepting cookies box is checked (Figure 6). Click **OK**.

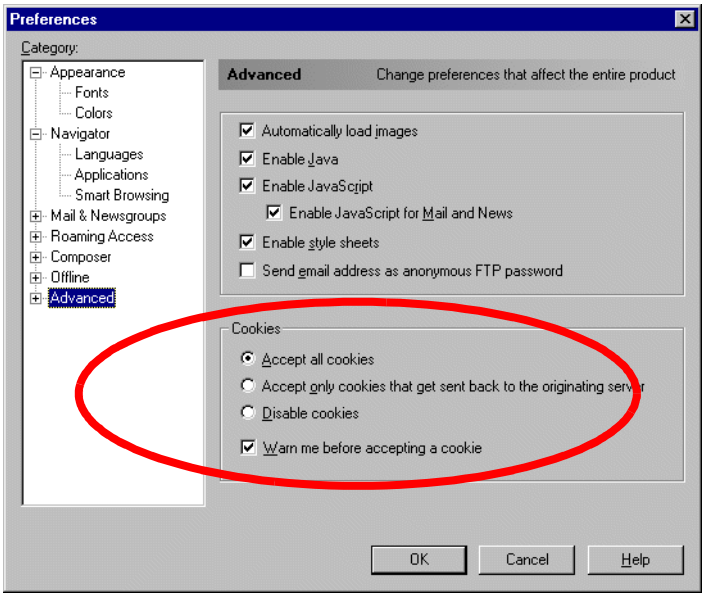

Figure 6. Editing Netscape to accept cookies

__ 5. You now want to test the Domino Web application by entering the following URL (remember to replace *xx* with your team number):

```
http://PWDI.PID.IBM.COM:80xx/DomWASLab.nsf/loanapp?openform
```

You should now see your Domino loan application shown in Figure 7. Notice that the name field is automatically filled in with the Anonymous value. Since you have not enabled security, Domino does not know who you are.

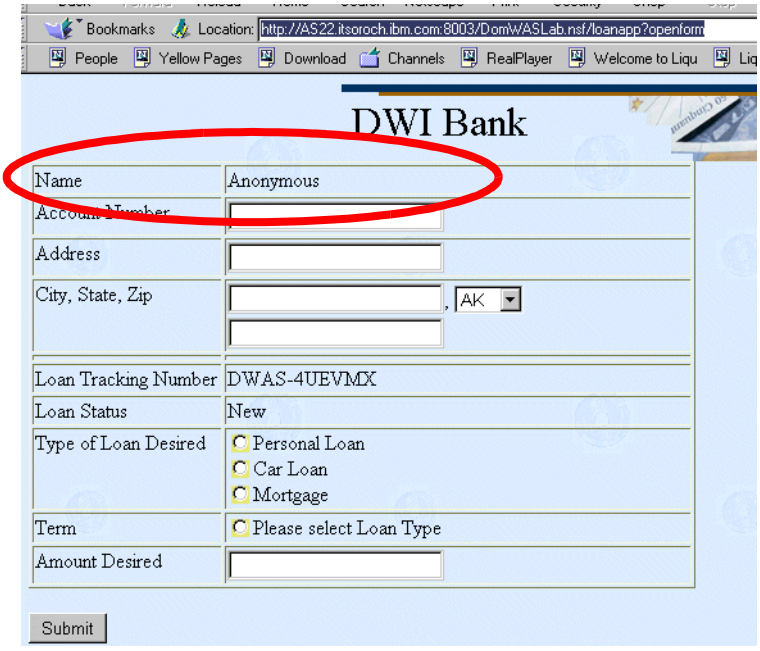

Figure 7. Accessing Domino loan application from a Web browser

__ 6. Close the Netscape browser window.

Lab 2. Creating a simple Web application

In this exercise, you create an instance of a WebSphere Application Server V3.5.2 for iSeries for your team and place a simple Java servlet onto it.

Objectives

This lab teaches you how to:

- Create an instance of the WebSphere Application Server.
- Configure Lotus Domino for AS/400 as HTTP server for WebSphere.
- Modify and compile a simple Java servlet on the iSeries server.
- Create a Web Application.
- Test whether you can access the servlet from a Web browser.

Important

Throughout these lab exercises, replace *xx* with your team number. Also, refer to Table 1 on page 4 to ensure that the correct values for the configuration parameters are entered.

Task 1: Creating an instance of the WebSphere Application Server

In this task, you create a new instance of the WebSphere Application Server 3.5.2 administrative server. Each team configures and uses resources that are independent of one another. This is useful in other scenarios as well, such as having multiple versions of the same application running simultaneously on the same iSeries 400 or AS/400 server for development purposes.

Important: The WebSphere instance for each team has already been created and started to save some time during the lab. Please continue with “Verifying the WebSphere Application Server 3.5.2 instance was started” on page 18 now.

Creating your WebSphere Application Server 3.5.2 instance

Perform the following tasks to create your WebSphere Application Server 3.5.2 instance:

__ 1. Creating a WebSphere instance is easy, there’s a Java program that comes with WebSphere which does everything for you. Enter the OS/400 Qshell Interpreter and run the script that creates all new server directories and sets up the correct authorities. In the 5250 emulation session, start the Qshell Interpreter by entering either the `STRQSH` or `QSH` command into the OS/400 command line.

__ 2. In the Qshell environment, enter the following command (in a single line) to create your instance of a WebSphere Application Server 3.5.2. Make sure to replace *xx* with your *team number*:

```
/QIBM/ProdData/WebASAdv/bin/crtnewinst -instance WASxx
-bootstrap 9xx -lsd 90xx
```

__ 3. Wait for the script to complete. A dollar sign ($) appears when the script completes.

This script creates a directory structure within the OS/400 Integrated File System (IFS) under /QIBM/UserData/WebASAdv/WASxx as well as an SQL ccollection named WASxxREP. The directory is used to store all the objects necessary for your new WebSphere Application Server instance and the SQL collection contains all configuration parameters.

Starting your WebSphere Application Server 3.5.2 instance

Perform the following tasks to start your server instance:

__ 1. At this point, verify that you did everything correctly. To do this, start your new WebSphere instance by typing the following command on the Qshell environment command line:

```
/QIBM/ProdData/WebASAdv/bin/strwasinst -instance WASxx
```

__ 2. The script for starting your new instance of WebSphere Application Server 3.5.2 (`strwasinst`) runs for several minutes. However, you may press F12 to exit the Qshell environment while the script continues running in the background. **Tip:** If you use F12 (rather than F3), to disconnect from Qshell, you will be able to still see the messages and commands later when you start Qshell again.

Verifying the WebSphere Application Server 3.5.2 instance was started

To verify that your server instance was started, enter the following command on an OS/400 command line:

```
WRKACTJOB SBS(QEJBSBS)
```

You should see the jobs WASxxMNTR and WASxxADMN (where *xx* is your team number) for your WebSphere instance.

Note: You will see other jobs running in this subsystem, including the default server and those WebSphere instances created by other student teams.

It takes some time for your server jobs to become ready because this is the first time you are starting your server and a default configuration must be created. Although you may continue with the next task, be aware that the WebSphere Applications Server is not ready until you verify it as described later in this lab (“Testing your new configuration” on page 20).

Task 2: Configuring Domino for AS/400 as an HTTP server for WebSphere

Up to this point, you have used the HTTP server of Lotus Domino for AS/400 only to serve Domino databases. For this and the following labs, you also want to be able to serve Web applications running under the control of the WebSphere Application Server 3.5.2 server on an iSeries 400 or AS/400 server.

Modifying the Domino Server document of your Domino server

Perform the following tasks to modify the Domino Server document of your Domino server:

__ 1. In your Domino Administrator (or Notes Client), open the Domino Directory (file names.nsf - formerly called the Names and Address Book (NAB) or Public Address Book (PAB)) on the Domino server for your team (DOMWASxx).

__ 2. Expand the “Server” folder and open the “Servers” view.

__ 3. Edit the Domino Server document for your Domino server (DOMWASxx).

__ 4. In the Domino Server document, click the **Internet Protocols** tab and then click the **HTTP** tab. In the middle of the right column, in the DSAPI filter file names field, enter the following file name:

```
/qsys.lib/qejb.lib/domino.srvpgm
```

See Figure 8.

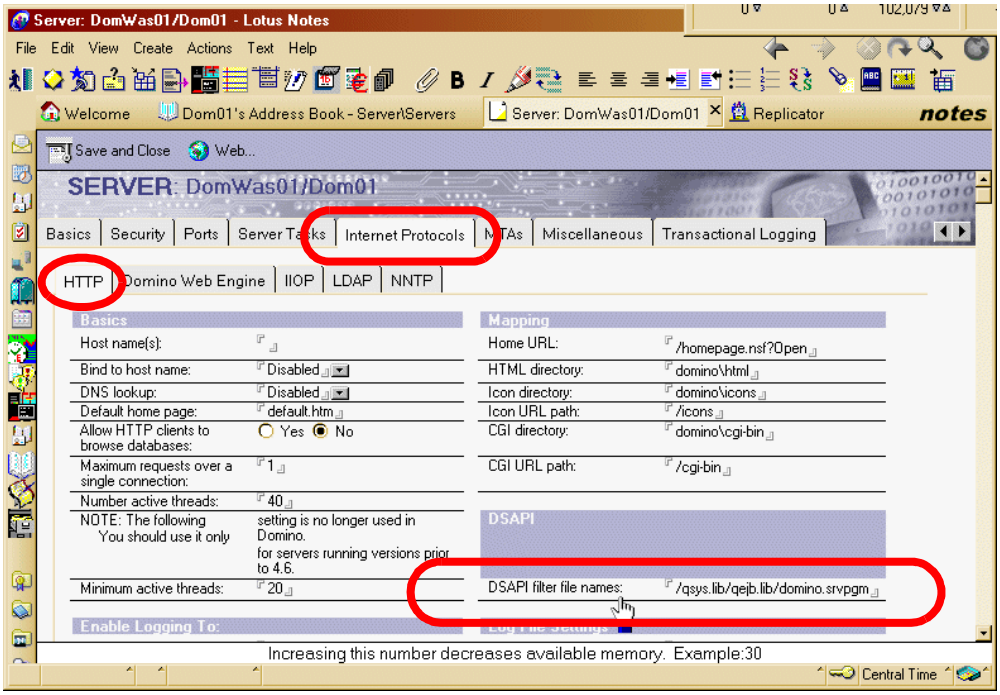

Figure 8. Define DSAPI filter file name

__ 5. Click the **Save and Close** button to exit the Domino Server document.

Modifying the notes.ini file of your Domino server

Perform the following tasks to modify the notes.ini file of your Domino server:

__ 1. In your 5250 emulation session you should still see the *Work with Domino Servers* panel. If not, enter the following command on the OS/400 command line and press Enter:

```
WRKDOMSVR DOMWASxx
```

__ 2. Enter option `6` (End Server) in the Opt field next to *your* Domino server (DOMWASxx). Make sure you select the correct Domino server, with *xx* being your team number and press Enter.

The “Confirm Ending the Domino Server” display appears. Verify that it is actually *your* Domino server, and press Enter to confirm ending it.

Press F5 to refresh your display (you may have to do this several times) and verify that the status of your Domino server is changed to *ENDED before continuing to the next step.

__ 3. Once the Domino server is ended, enter option `13` (Edit NOTES.INI) in the Opt field next to your Domino server (DomWASxx) and press Enter.

__ 4. On the “Edit file” display, scroll down to the bottom of the file and enter the letter `i` in the CMD field next to the last line in the file and press Enter. A new line is inserted after the one were you entered the letter “i”.

__ 5. Enter the following statement into the new line:

```
WebSphereInit=/qibm/UserData/WebASAdv/WASxx/properties/
bootstrap.properties
```

The string needs to be entered as a single line. Again, make sure you enter your team number in place of the *xx* in the middle of the string as part of WASxx. Press F3 twice to exit and save the updated notes.ini file.

__ 6. Restart your Domino server by entering option `1` (Start Server) in the Opt field next to your Domino server (DomWASxx) and press Enter.

__ 7. Once your Domino server is started, restart your Domino HTTP server task. Type option `8` (Work console) in the Opt field next to *your* Domino server (DOMWASxx) and press Enter. From the Domino console, enter the following Domino command on the command line and press Enter:

```
load http
```

This starts the Domino HTTP server task (verify that it started successfully). If you see an error message instead, you should check your configuration changes you made at step __ 4. on page 19 or __ 5. on page 20 for any typographical errors.

__ 8. Press F3 to exit the Domino console display.

__ 9. Update OS/400 authorities. Enter the following command on the OS/400 command line to grant the QNOTES user profile the authority required for creating the necessary WebSphere Application Server log files:

```
CHGAUT '/QIBM/UserData/WebASAdv/WASxx/logs' USER(QNOTES) DTAAUT(*RWX)
```

You may also just type the command `CHGAUT` and then press F4 (Prompt), to reduce typing effort.

Testing your new configuration

Now that the WebSphere instance is configured and started, you need to test it by running the “Snoop” servlet. Perform the following tasks:

__ 1. Make sure both your WebSphere monitor job (WASxxMNTR) and the administrative server job (WASxxADMN) for your team are running and in the correct states. You cannot continue until they are ready. To check this, perform the following tasks:

a. Enter the Work with Active Jobs (WRKACTJOB) command to verify that they are in JVAW and EVTW status:

```
wrkactjob sbs(qejbsbs)
```

b. Display the joblog for the WASxxADMN administrative server job. From the WRKACTJOB display, enter option `5` (Work with) next to the WASxxADMN job. Press Enter.

c. On the Work with Job display, enter option `10` (Display job log, if active or on job queue) to display the joblog. Press Enter.

d. Look for the following message:

```
WebSphere administration server WASxxADMN ready.
```

You may have to press F5 several times to refresh the display. Scroll down if “More...” appears in the lower right corner of your display.

e. Position the cursor on the ready message and press F1 to verify the administration server is listening to the correct port assigned to your team (9xx) and that the message is new (look at the time stamp). See Figure 9.

```
                        Additional Message Information

Message ID . . . . . :   EJB0106       Severity . . . . . :   00
Message type . . . . . :   Information
Date sent  . . . . . :   02/18/01      Time sent  . . . . . :   11:13:53

Message . . . . :   WebSphere administration server WASxxADMN ready.
Cause . . . . . :   WebSphere administration server WASxxADMN is ready to
  handle requests from the WebSphere administration console on port 9xx.
  Diagnostic information is controlled on port 20834.
```

Figure 9. WebSphere administration server started successfully

__ 2. Press F3 to exit and return to the Work with Active Jobs display.

Important: The WebSphere administrative console for each team may have already been started by your instructor to save some time during the lab. If that is the case, click the blue icon on the Windows task bar to open its window and continue with “Define the port for your WebSphere virtual host (default_host)” on page 22 now.

__ 3. Start the WebSphere administrative console and connect it to your WebSphere instance. To do this, bring up a DOS prompt on your PC client and type in the following commands:

```
C:\>cd \WebSphere\Appserver\bin\    <Press Enter>
C:\WebSphere\Appserver\bin\>adminclient PWDI 9xx     <Press Enter>
```

Be sure to type the host name (PWDI) in upper case[1] and use the correct administrative server port (9xx).

__ 4. The console takes some time to start. You may see the panel shown in Figure 10 for several seconds or even minutes.

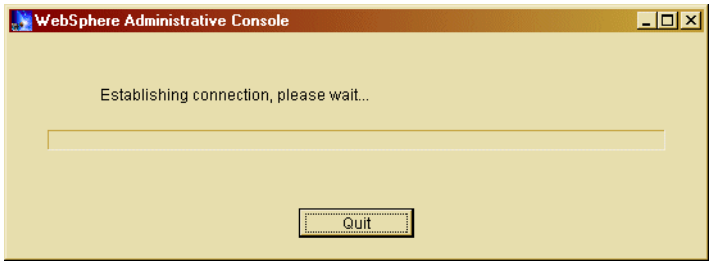

Figure 10. WebSphere Administrative Console establishing connection

__ 5. The text eventually changes to “loading” and you see the Administrator console shown in Figure 11 on page 22.

Note: The console is still not ready yet. Wait until you see the “Console Ready” message in the lower pane and a plus sign (+) next to WebSphere

[1] In fact, the case must be the same as defined in the OS/400 TCP/IP configuration (CFGTCP option 12 or CHGTCPDMN).

Administrative Domain in the left pane. You have one final step to do before you can use servlets in your configuration.

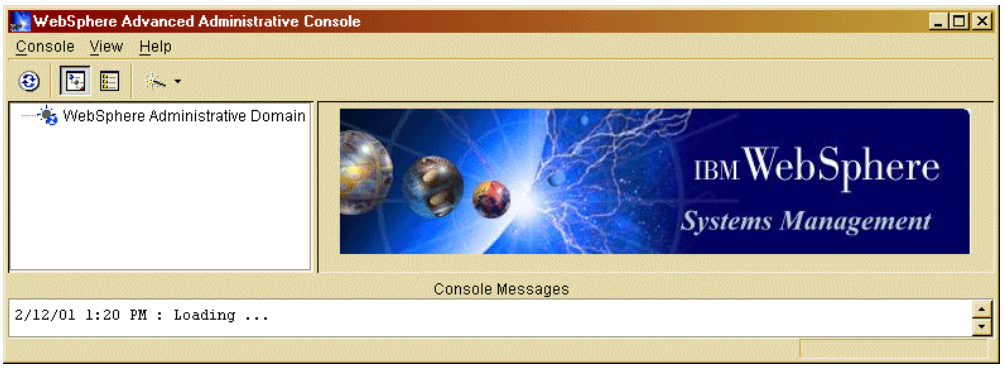

Figure 11. WebSphere Console still loading

Define the port for your WebSphere virtual host (default_host)

Perform the following steps to define the port for your WebSphere virtual host to recognize your HTTP port number:

__ 1. Expand the tree under the WebSphere Administrative Domain node (click the **+** sign).

__ 2. Click on **default_host**.

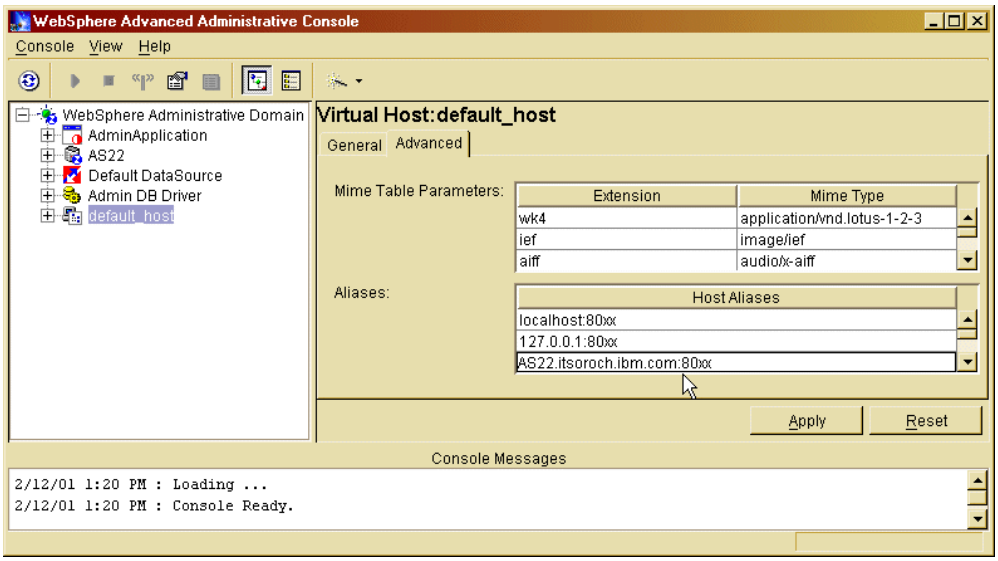

Figure 12. WebSphere Administrator Console Advanced Tab for default_host

__ 3. As shown in Figure 12, click the **Advanced** tab in the right-hand pane. Add the HTTP port number `:80xx` (don't forget the colon and be sure to replace the *xx* with your team number) to every hostname listed in the Aliases field. You may need to scroll down to see all of the host names. Be sure you do *not* modify the host names and IP addressees.

Note: In case you accidently change or delete an entry, press Esc to restore the old value.

Click **Apply** to save your changes and wait until you see a message on the Console Messages pane similar to:

```
Command "default_host.ModifyAttributes" completed successfully.
```

__ 4. Select the node that has the same name as the iSeries or AS/400 server (PWDI). Click the plus sign (**+**) in front of the node to expand its topology.

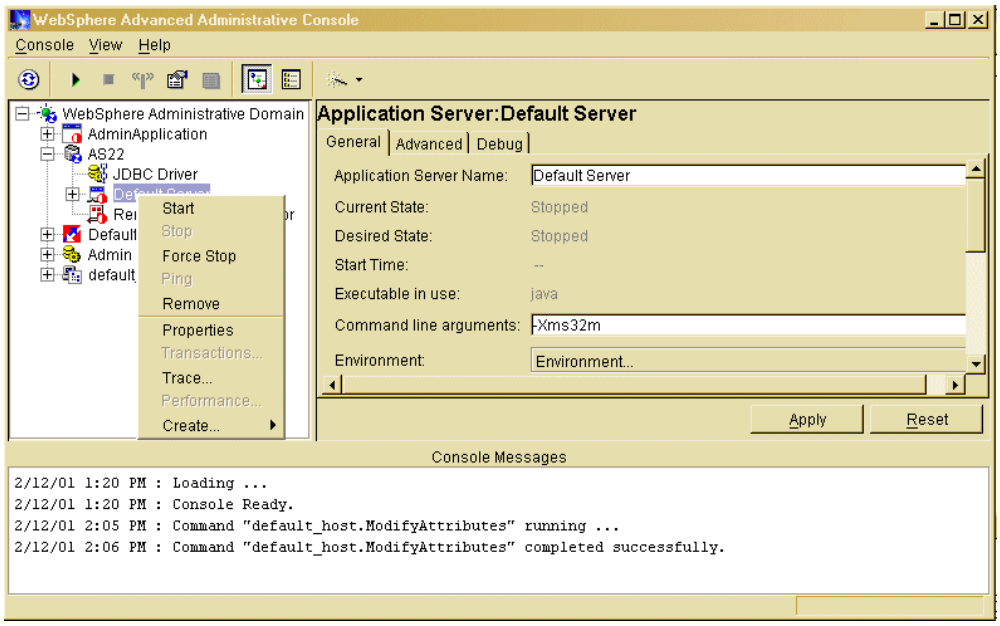

Figure 13. Start the Default Server

__ 5. Your instructor may have renamed the Default Server to **WASxxSRVR** to allow easier management of the servers for all students. Depending on that either right-click the **Default Server** or **WASxxSRVR** and select **Start** as shown in Figure 13. Wait until a pop-up window appears (Figure 14) that tells you the server has started. If the default server is already started, stop it and then restart it.

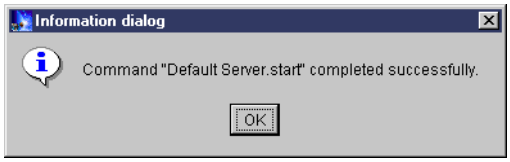

Figure 14. Default Server started successfully message

__ 6. Copy the Snoop servlet (SnoopServlet.class) from the production directory to your team directory structure. It is located in the directory:

```
/qibm/proddata/webasadv/hosts/default_host/default_app/servlets
```

Copy the SnoopServlet.class file to the servlets directory of *your* WebSphere instance of the WebSphere Application Server 3.5.2:

```
/qibm/userdata/webasadv/Wasxx/hosts/default_host/default_app/servlets
```

To do this, enter the following OS/400 command in a single line:

```
wrklnk
'/qibm/userdata/webasadv/Wasxx/hosts/default_host/default_app/servlets'
```

(You may also start with the command wrklnk '/qibm' and enter a 5 in front of each directory name shown in the path above, to avoid typing errors)

__ 7. Enter option `11` (Change Current Directory) next to the Servlets directory and press Enter. Press F3 to exit the Work with Links panel.

__ 8. Issue the following OS/400 command:

```
wrklnk '/qibm/proddata/webasadv/hosts/default_host/default_app/servlets'
```

Enter option `5` (Display) next to the Servlets directory and press Enter.

__ 9. Enter option `3` (Copy) next to the SnoopSerlvet.class file and press Enter. This copies the Snoop servlet from the production directory to the current directory which you just set to your WebSphere instance.

__ 10. Test the servlet by starting your Netscape Web browser and enter the following URL:

```
http://PWDI.PID.IBM.COM:80xx/servlet/snoop
```

The Web page shown in Figure 15 should appear.

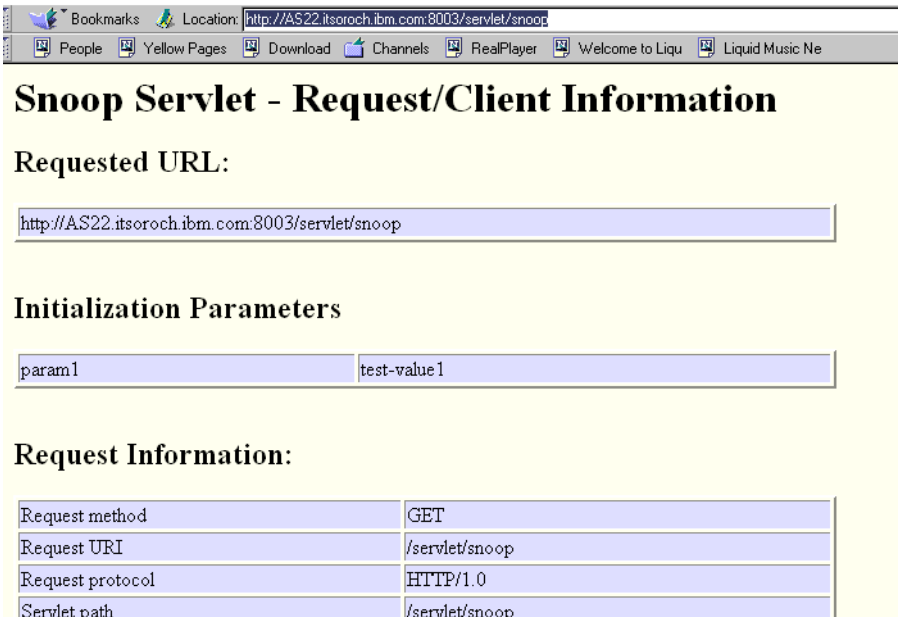

Figure 15. Snoop servlet

Once you have successfully configured your WebSphere instance, you are ready to try installing servlets, Java ServerPages (JSPs), and Enterprise JavaBeans (EJBs). For the purpose of this lab, you create a simple servlet to learn how security can be implemented, how to switch between WebSphere resources and Domino applications, and how to use the Single Sign-On capability between WebSphere and Domino.

Task 3: Modifying and compiling a simple Java servlet on the iSeries server

Because it is *not* the objective of this lab to perform any kind of application development, we included a very simple servlet as an example for a Web application. The Java code for our simple servlet is shown here:

```
import java.io.*;
import java.util.*;
import javax.servlet.http.*;
import java.math.*;
import com.ibm.as400.access.*;
```

```
public class SimpleServlet extends javax.servlet.http.HttpServlet {
/**
 * method name: copyItems
 * parms: none
 * description:
 *default constructor, not of any importance.
 *
 */
public SimpleServlet() {
super();
}
/**
 * method name: doGet
 * parms:  1-request object
 *  2-response object
 * description:
 *code for a GET action.
 *
 * Creation date: (12/11/2000 1:55:32 PM)
 * @param req javax.servlet.http.HttpServletRequest
 * @param res javax.servlet.http.HttpServletResponse
 */
public void doGet(HttpServletRequest req, HttpServletResponse res)
throws javax.servlet.ServletException, java.io.IOException
{
PrintWriter out = res.getWriter();
HttpSession session = req.getSession(true);

res.setContentType("text/html");
out.println("<title>SimpleServlet</title><body>");

out.println("<br>Click <b><a href=\""+DOMINO_URL+"\">HERE</a></b> to visit the Domino
page<br>");

displayJavaInfo(out, req);
displayAS400Info(out, req);

out.println("</body>");

}// doGet(..)

// the following static variables are used in generating table html
private final static java.lang.String COL1_ATTS = "<TR VALIGN=top><TD WIDTH=\"325\"><B><FONT
COLOR=\"0000FF\">";
private final static java.lang.String COL1A_ATTS = "<TR VALIGN=top><TD WIDTH=\"100\"><B><FONT
COLOR=\"FF0000\">";
private final static java.lang.String COL2_ATTS = "</FONT></B></TD><TD WIDTH=\"213\"><B>";
// the following three strings need to be changed to match the system the servlets runs on.
private final static java.lang.String HOST = "MyHOST.ourdomain.com";
private final static java.lang.String NL = "\n";
private final static java.lang.String PASSWORD = "MyPwd    ";
private final static java.lang.String ROWEND_ATTS = "</B></TD></TR>\n";
private final static java.lang.String USERID = "Kurtis    ";

/**
 * method name: displayAS400Info
 * parms:  1-output print stream
 *  2-servlet request object
 * description:
 *generates html for all system values from the respective AS/400.  makes use
 *of the AS/400 toolkit classes.
 *
 * Creation date: (2/8/2001 10:27:47 PM)
 * @param out java.io.PrintWriter
 * @param req javax.servlet.http.HttpServletRequest
 */
public void displayAS400Info(PrintWriter out, HttpServletRequest req)
{

out.println("<h1>AS/400 System Values for host system "+HOST+"</h1>");

AS400 as400 = new AS400(HOST,USERID, PASSWORD);

if (as400 != null) {

// host, userid and password are valid so we can generate table for system values
out.println("<form><table boarder=0 cellspacing=0 cellpadding=0>");
try {
```

```
// generate a dynamic collection (vector) of all system values
SystemValueList svl = new SystemValueList(as400);
Vector v = svl.getGroup(SystemValueList.GROUP_ALL);

SystemValue sysval = null;
Enumeration e = v.elements();
// interate through all possible system values.
while (e.hasMoreElements()) {
  sysval = (SystemValue)e.nextElement();
  out.println(
   COL1A_ATTS+sysval.getName()
  +COL1B_ATTS+sysval.getDescription()
  +COL2_ATTS+strVal(sysval)+ROWEND_ATTS
  );

}

// close the table and the form
out.println("</table></form>");

}
catch (Exception e){
// must have run into a problem with the system values.
out.println ("SystemValue Exception: " + e.getMessage());
}

}
else {
// something wrong with host, userid and/or password
out.println("<h1>AS/400 access error, host="+HOST+" userid="+USERID+" password="+PASSWORD);
}

}

/**
 * method name: displayJavaInfo
 * parms:  1-output print stream
 *  2-servlet request object
 * description:
 *generates html for all some Java Virtual Machine values.
 *
 * Creation date: (2/8/2001 10:27:29 PM)
 * @param out java.io.PrintWriter
 * @param req javax.servlet.http.HttpServletRequest
 */
public void displayJavaInfo(PrintWriter out, HttpServletRequest req)
{
out.println("<h1>Java Virtual Machine information</h1>");

// the System object has most of the information
out.println(
"<form>"
+"<table boarder=0 cellspacing=0 cellpadding=0>"
+COL1_ATTS+"Remote user:"+COL2_ATTS+req.getRemoteUser()+ROWEND_ATTS
+COL1_ATTS+"Runtime Environment
version:"+COL2_ATTS+System.getProperty("java.version")+ROWEND_ATTS
+COL1_ATTS+"Runtime Environment
vendor:"+COL2_ATTS+System.getProperty("java.vendor")+ROWEND_ATTS
+COL1_ATTS+"Class format version
number:"+COL2_ATTS+System.getProperty("java.class.version")+ROWEND_ATTS
+COL1_ATTS+"Operating system name:"+COL2_ATTS+System.getProperty("os.name")+ROWEND_ATTS
+COL1_ATTS+"Operating system
architecture:"+COL2_ATTS+System.getProperty("os.arch")+ROWEND_ATTS
+COL1_ATTS+"Operating system version:"+COL2_ATTS+System.getProperty("os.version")+ROWEND_ATTS
+COL1_ATTS+"User's account name:"+COL2_ATTS+System.getProperty("user.name")+ROWEND_ATTS
 +COL1_ATTS+"User's home directory:"+COL2_ATTS+System.getProperty("user.home")+ROWEND_ATTS
 +COL1_ATTS+"User's current working
directory:"+COL2_ATTS+System.getProperty("user.dir")+ROWEND_ATTS
);

// use a dropdown control to display the classpath
out.println(
 COL1_ATTS+"Class path:"+COL2_ATTS
+"<select name=\"classpath\">"
);

// get fancy and split classpath into separate directories/files.
```

```
StringTokenizer st = new StringTokenizer(System.getProperty("java.class.path"), ":");
while(st.hasMoreTokens()) {
out.println("<option>"+st.nextToken());
}

// close select, table and the phantom form
out.println("</select>"+ROWEND_ATTS+"</table></form>");
}

/**
 * method name: strVal
 * parms:  1-SystemValue object to get
 *
 * description:
 *returns a string value representing the value of the passed SystemValue object.
 *a SystemValue object value can be complex and a simple Java cast to String type
 *does not work.
 *
 * Creation date: (2/9/2001 11:59:34 AM)
 * @return java.lang.String
 * @param o java.lang.Object
 */
private String strVal(SystemValue sv) {
String rval = "*error";

try {
switch(sv.getType()) {

case SystemValueList.TYPE_ARRAY:
// The data contained by this system value is a String[] object.
String t[] = (String[])sv.getValue();
rval = "";
for (int i=0; i<t.length; i++) {
if (i>0)
rval+=":"+t[i];
else
rval=t[i];
}
break;

case SystemValueList.TYPE_DATE :
// The data contained by this system value is a Date object.
rval = ((Date)sv.getValue()).toString();
break;

case SystemValueList.TYPE_DECIMAL:
// The data contained by this system value is a BigDecimal object.
rval = ((BigDecimal)sv.getValue()).toString();
break;

case SystemValueList.TYPE_INTEGER:
// The data contained by this system value is an Integer object.
rval = ((Integer)sv.getValue()).toString();
break;

case SystemValueList.TYPE_STRING:
// The data contained by thissystem value is a String object.
rval = (String)sv.getValue();
break;

default:
rval = "*unknown datatype";
break;
}
}
catch (Exception e){
System.out.println ("strVal()-->Exception: " + e.getMessage());
}
return rval;
}

private final static java.lang.String COL1B_ATTS = "</FONT></B></TD><TD
WIDTH=\"325\"><B><FONT COLOR=\"0000FF\">";
private final static java.lang.String DOMINO_URL = "http://www.ibm.com";
}
```

You are required to perform a few modifications during this lab. These modifications are primarily for enabling this servlet to work in an environment where multiple students are performing the same tasks on a single system.

To keep this lab simple and focused on the topic of Domino & WebSphere Integration, you perform the modifications through an OS/400 user interface. In a real environment, you would likely develop the Web Application on your workstation using tools such as VisualAge for Java and deploy it through WebSphere Studio.

Modifying the source code for SimpleServlet

The source code for this servlet is stored in the /DomWasLab/Examples/xx directory (where *xx* is your team number) of the OS/400 Integrated File System (IFS) of your iSeries 400 or AS/400 server (PWDI). To modify and compile the source code, perform the following tasks:

__ 1. From 5250 emulation session, enter the following command (replace *xx* with your team number):

```
wrklnk '/DomWasLab/Examples/xx'
```

__ 2. Enter option `5` (Display) in the Opt Field next to the number of your team (xx). Press Enter.

__ 3. Enter option `2` (Edit) in the Opt Field next to the SimpleServlet.java filename. Press Enter to edit the source code.

Note: This ability was introduced in OS/400 V4R5. For previous releases, you have to use the Edit File (`EDTF`) command.

__ 4. In the Control: field, enter in the word `HOST` (all uppercase) as shown in Figure 16. Press F16 (shift F4 function key) to search for that string.

```
 Edit File: /qibm/UserData/WebASAdv/WASxx/servlets/SimpleServlet.java
Record . :      53 of     229 by  10                    Column:    1 of   81 by 126
Control  : HOST

CMD ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+....0....+....1....+....2....
    private final static java.lang.String HOST = "MYHOST.ourdomain.com";
    private final static java.lang.String NL = "\n";
    private final static java.lang.String PASSWORD = "MyPwd";
    private final static java.lang.String ROWEND_ATTS = "</B></TD></TR>\n";
    private final static java.lang.String USERID = "Kurtis   ";

   /**
    * method name: displayAS400Info
    * parms:    1-output print stream
    *      2-servlet request object
    * description:
    *    generates html for all system values from the respective AS/400.  makes use
    *    of the AS/400 toolkit classes.
    *
    * Creation date: (2/8/2001 10:27:47 PM)
    * @param out java.io.PrintWriter
    * @param req javax.servlet.http.HttpServletRequest
    */


F2=Save  F3=Save/Exit   F12=Exit   F15=Services   F16=Repeat find   F17=Repeat change   F19=Left   F20=Right
```

Figure 16. Editing the example code for the SimpleServlet servlet

__ 5. In the first line of the Edit File panel (Figure 16), replace the MYHOST.ourdomain.com string with:

```
PWDI.PID.IBM.COM
```

This is the host name of the iSeries 400 or AS/400 server for the lab. Make sure you do not delete the apostrophes or the semicolon at the end of the line.

__ 6. In the third line, replace the word MyPwd with your OS/400 user ID password that you are using in this lab (`dom2was`). Make sure you delete all the extra spaces (do *not* delete the apostrophes and the semicolon at the end of the line).

__ 7. In the fifth line, replace the word Kurtis with the name of the OS/400 user ID profile (`DOMWASxx`). Make sure you delete all the extra spaces (do *not* delete the surrounding apostrophes and the semicolon at the end of the line).

__ 8. In the Control: field, type in the word `DOMINO_URL` (all uppercase) and press F16 (shift F4 function key) to search for that string.

__ 9. The second to last line of the file should be shown on your display. Change the URL `http://www.ibm.com` to the URL of the Domino application created in Lab 1. “Developing a Domino application” on page 9. The correct URL is:

```
http://PWDI.PID.IBM.COM:80xx/DomWASLab.nsf/LoanApp?OpenForm
```

Again, make sure you do *not* delete the surrounding apostrophes (") and the semicolon (;) at the end of the line.

__ 10. Press F3 twice to save the changed file and exit the Edit File utility.

Creating the default directory structure for a new Web application

When you create a new Web application, a default directory structure is assumed to store the executable code in. You now create the directory structure for the Web application used in this lab.

__ 1. Enter the following OS/400 command and press Enter:

```
wrklnk '/qibm'
```

__ 2. Enter option `5` (Display) next to qibm and press Enter.

__ 3. Enter option `5` (Display) next to UserData and press Enter.

__ 4. Enter option `5` (Display) next to WebASAdv and press Enter. You may need to scroll down one page to find WebASAdv.

__ 5. Enter option `5` (Display) next to WASxx and press Enter. Here, *xx* is your team number. You may need to scroll down one or more pages to find WASxx.

__ 6. Enter option `5` (Display) next to hosts and press Enter.

__ 7. Enter option `11` (Change Current Directory) next to default_host and press Enter to make *default_host* your current directory.

__ 8. Enter the following command on the OS/400 command line and press Enter:

```
md DomApp
```

__ 9. Enter option `5` (Display) next to default_host and press Enter.

__ 10. Enter option `11` (Change Current Directory) next to DomApp and press Enter.

__ 11. Enter the following command on the OS/400 command line and press Enter:

```
md servlets
```

__ 12. Enter option `5` (Display) next to DomApp and press Enter.

__ 13. Enter option `11` (Change Current Directory) next to servlets and press Enter. This option changes your current directory to:

```
/qibm/UserData/WebASAdv/WASxx/hosts/default_host/DomApp/servlets
```

This is the directory for the servlets of the SimpleServlet Web application running under the control of your WebSphere Application Server 3.5.2 instance named *WASxx*.

Copying the source code to your servlets directory

To make it easier to compile the servlet, copy the file to the directory where the executable code needs to be created. Normally, you would not do this in a real world environment.

__ 1. Enter the following OS/400 command from a command line:

```
wrklnk '/DomWASLab/Examples/xx'
```

Here, *xx* represents your team number.

__ 2. Enter option `5` (Display) next to the xx directory and press Enter.

__ 3. Enter option `3` (Copy) in the Opt Field next to SimpleServlet.java and press Enter. This creates a copy of the SimpleServlet.java file in the current directory, which you just set to:

```
/qibm/UserData/WebASAdv/WASxx/hosts/default_host/DomApp/servlets
```

Press Enter to exit the *Work with Links* panel.

__ 4. Start ell by entering the following command on the OS/400 command line and press Enter:

```
qsh
```

__ 5. Start the compilation of the servlet by entering the following command on the Qshell command line:

```
/DomWasLab/Examples/jcomp xx
```

(Make sure to replace xx by your team number)

You will see a dollar sign ($) when the command is finished running. Press F12 to exit Qshell.

Tip: If you use F12, to disconnect form Qshell, you will be able to still see the messages and commands later when you start Qshell again.

__ 6. Verify that the class file (SimpleServlet.cls) for your new servlet has been created in directory:

```
/QIBM/UserData/WebASAdv/WASxx/hosts/default_host/DomApp/servlets
```

If you followed the instructions above, you should still see your directory, but you need to enter option 5 next to the *servlets* directory. If you do not see that directory, enter the `WRKLNK` command and press Enter.

Task 4: Creating a Web application

In this task you create a WebSphere Web Application to contain the SimpleServlet.

__ 1. If it is not already started, start your WebSphere Administrative console.

__ 2. Use the topology pane to move down the structure so you can select the ServletEngine. To do this, click the plus (**+**) sign next to the node with the name of the classroom system (PWDI). Then click the plus (**+**) sign next to *Default Server* (or **WASxxSRVR** if your instructor renamed the Default Server to that name).

__ 3. Right-click **DefaultServletEngine** and select **Create->Web Application** as shown in Figure 17.

Note: It takes a few seconds after you right-click before the Create Web Application window appears.

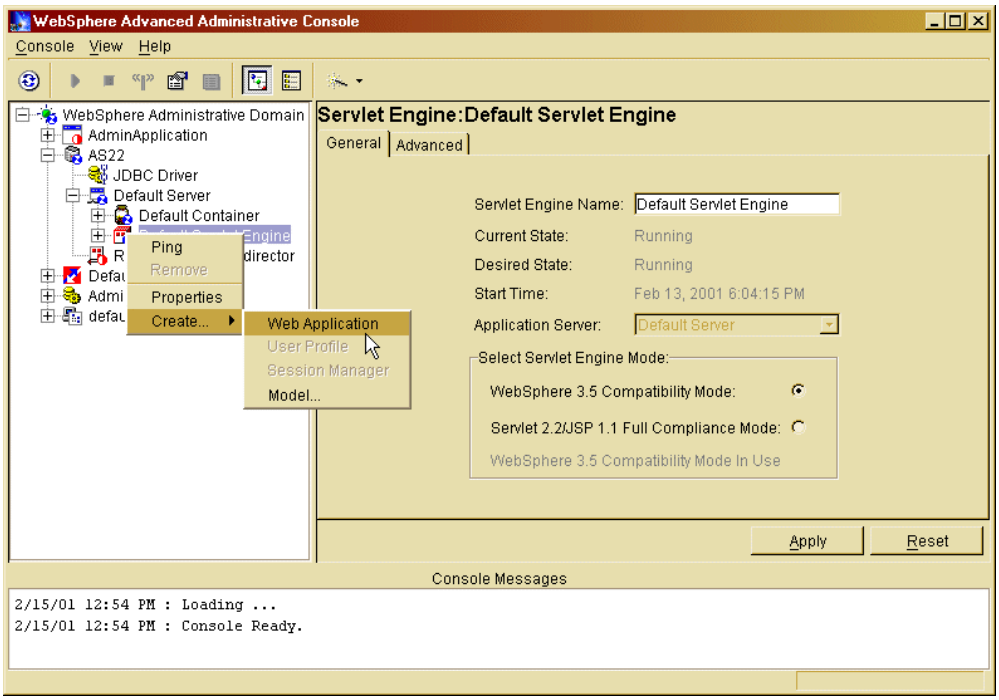

Figure 17. WebSphere Administrative Console: Create Web application

__ 4. The Create Web Application window appears as shown in Figure 18.

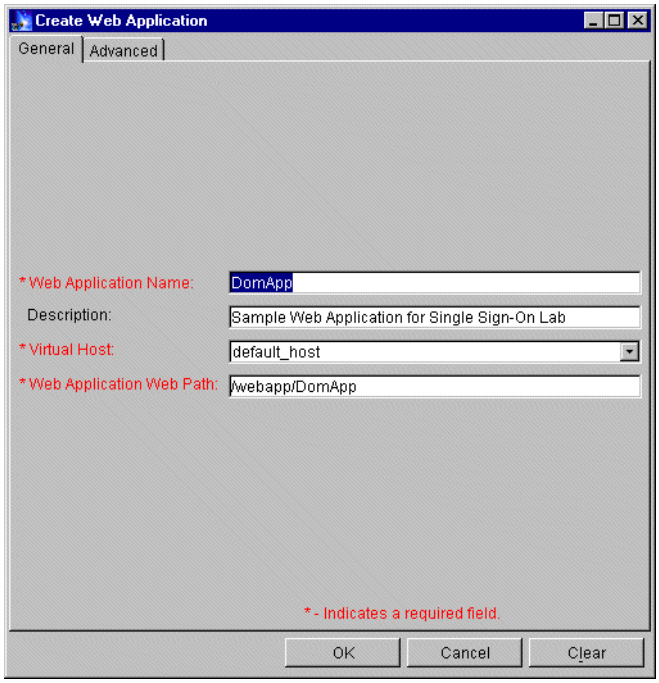

Figure 18. Create Web Application - General Tab

__ 5. Enter the following values:

- Web Application Name: `DomApp`
- Description: `Sample Web Application for Single Sign-On Lab`
- Virtual Host: default_host (leave the default)
- Web Application Web Path: `/webapp/DomApp`

__ 6. Click **OK** to create the Web Application. The panel shown in Figure 19 appears for several minutes. Wait until you see the information dialog box

window “Command "ServletGroup.create" completed successfully” and the same message in the Console Messages pane.

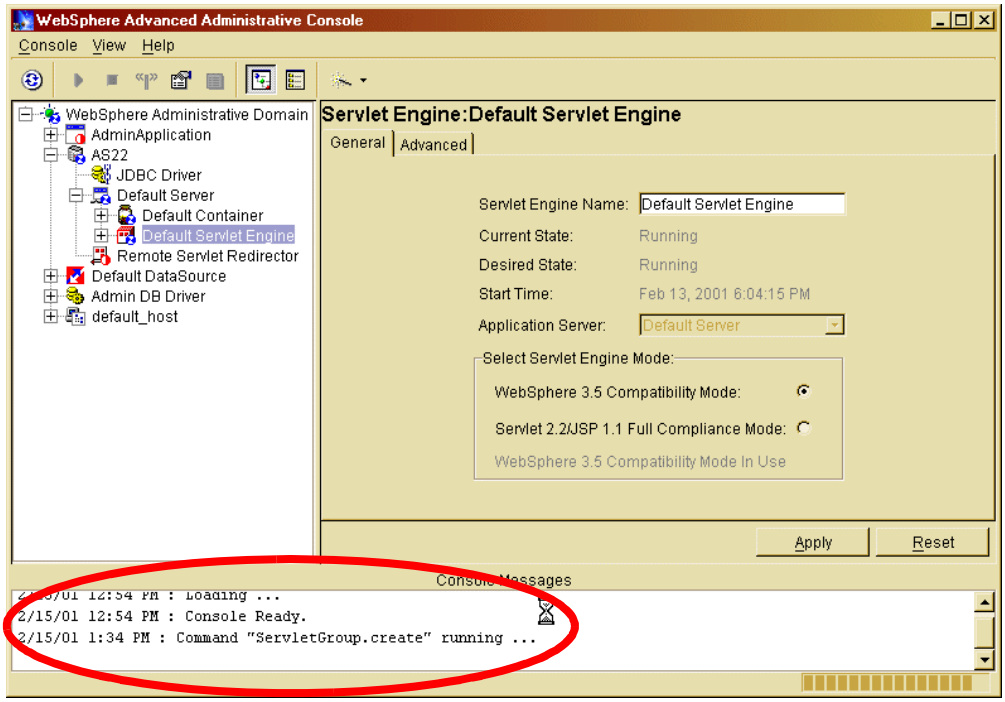

Figure 19. Create Web Application: ServletGroup.create running

__ 7. Click the plus sign (+) to *Default Servlet Engine* to expand the tree underneath it.

__ 8. Notice that you now have a *DomApp* application under the Default ServletEngine and that its icon is red, which indicates that it is not started.

__ 9. Click the **DomApp** application and then click the **Advanced** tab in the right pane.

__ 10. A panel similar to the one shown in Figure 20 appears. Verify the Classpath, which by default has been set to:

```
/qibm/userdata/webasadv/WASxx/hosts/default_host/DomApp/servlets
```

Remember this structure because it is where you must export your servlet.

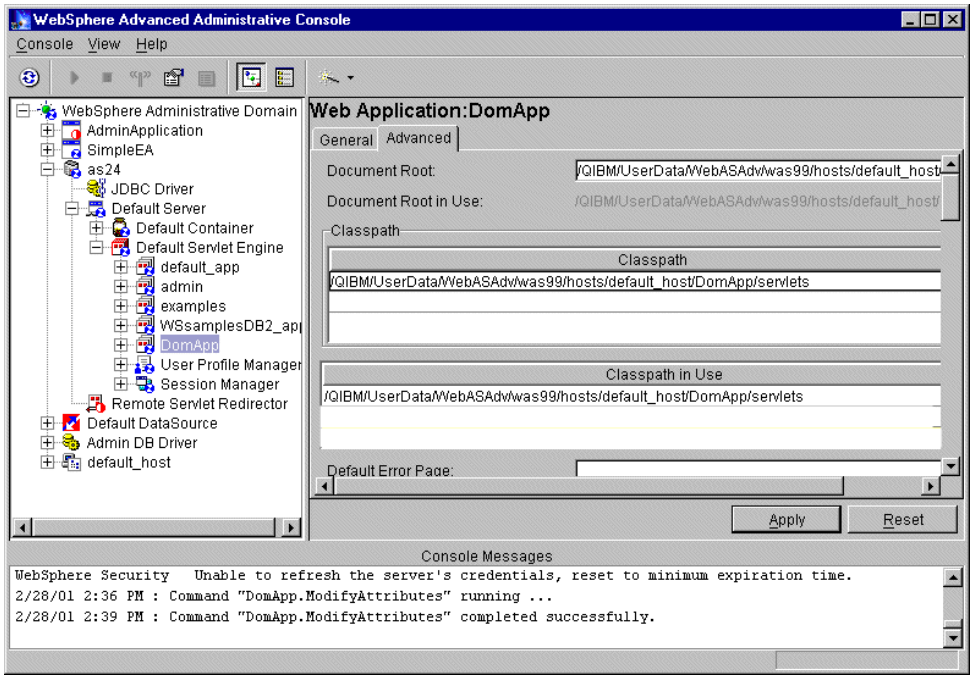

Figure 20. Web Application: DomApp - Advanced tab

__ 11. Now you need to add the JAR file for the Java Toolkit for AS/400 to the classpath. In the *Classpath* pane click in the first empty line under the class files directory as shown in Figure 21 and add the following path:

```
/qibm/ProdData/HTTP/Public/jt400/lib/jt400.jar
```

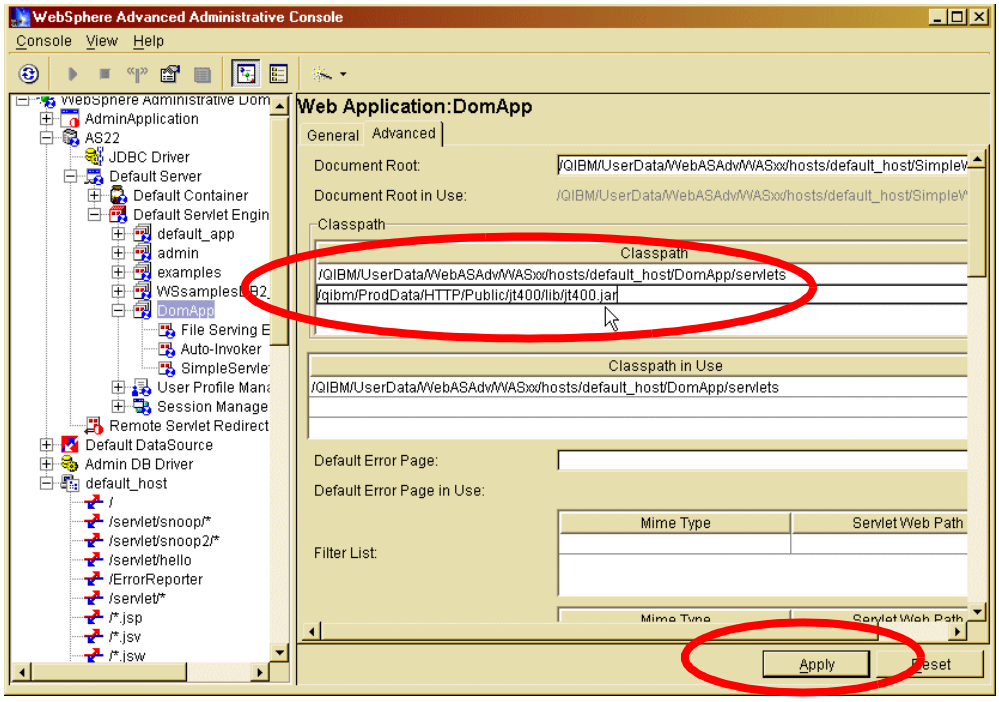

Figure 21. Web Application: Advanced tab - Add JT400.jar

__ 12. Click **Apply**.

__ 13. As shown in Figure 22, click on the **Wizards** icon in the menu bar to display its pull-down menu. Click **Add a Servlet**.

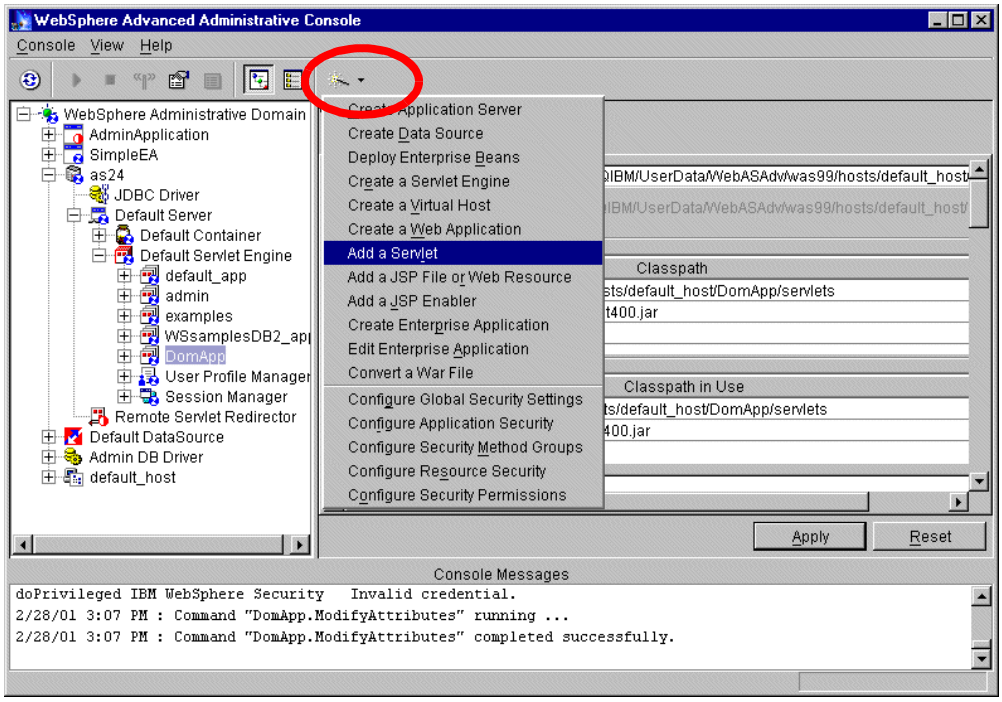

Figure 22. Web Application: DomApp - Add a Servlet

__ 14. On the Add a Servlet window, leave the default set to No and click **Next>** to continue (Figure 23).

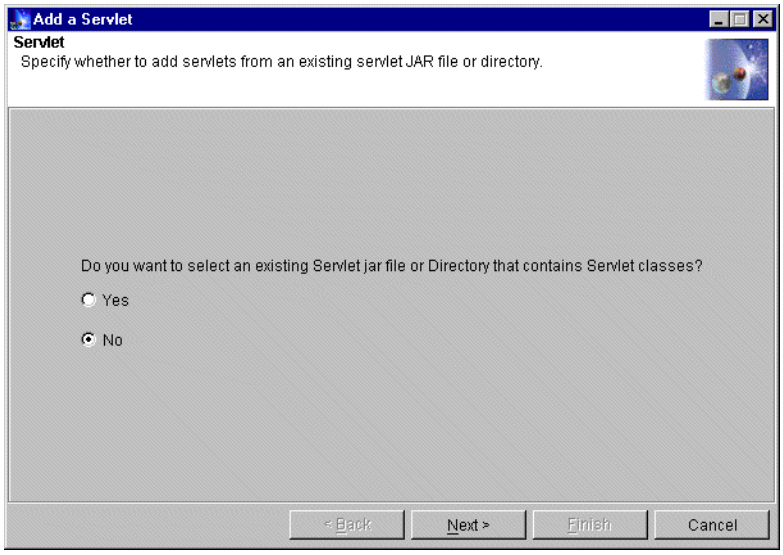

Figure 23. Adding a servlet window

__ 15. On the Select a Web application window, drill down until you can select the **DomApp** Web Application as shown in Figure 24. Please be patient and click each plus sign only once. For some branches, it may take several seconds to expand.

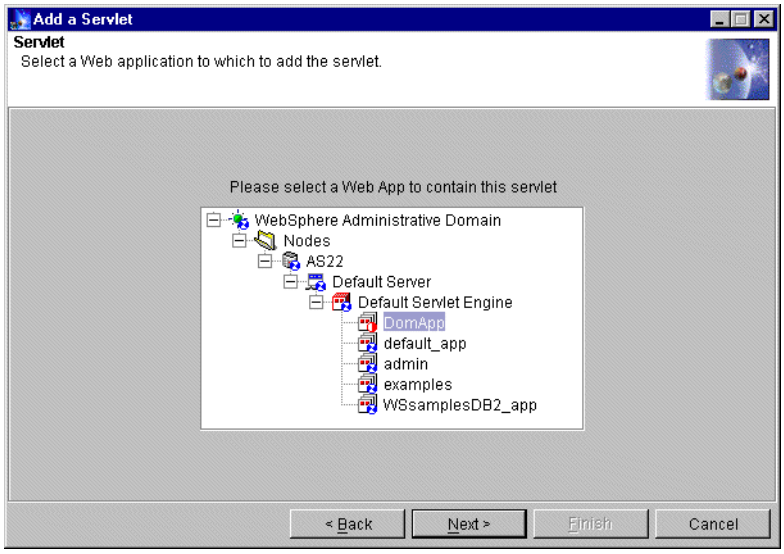

Figure 24. Select Web application to which to add servlet

__ 16. Click **Next>**.

__ 17. On the Select the Type of Servlet window, select **Create File-Serving Servlet** as shown in Figure 25.

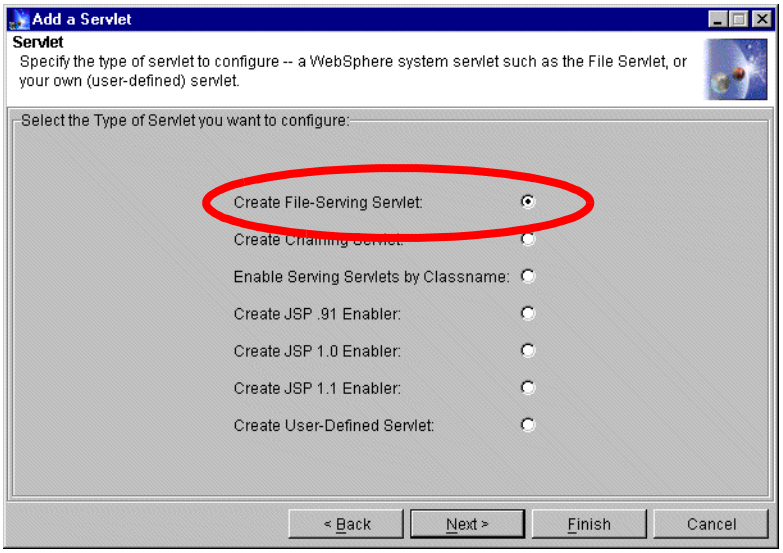

Figure 25. Type of servlet: Create File-Serving Servlet

__ 18. Click **Finish**.

__ 19. Wait until the window shown in Figure 26 appears and click **OK** Again, bepatient, this may take a couple of minutes.

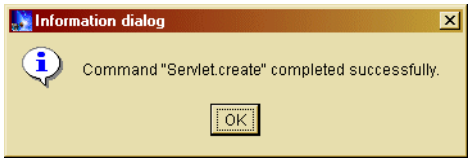

Figure 26. Web Application: SimpleWebApp - Servlet added successfully

__ 20. After the servlet is successfully created, repeat these steps. Start with step __ 13. on page 35 to add Enable Serving Servlets by Classname.

__ 21. Right-click on the **DomApp** application, and select **Create->Servlet** as shown in Figure 27.

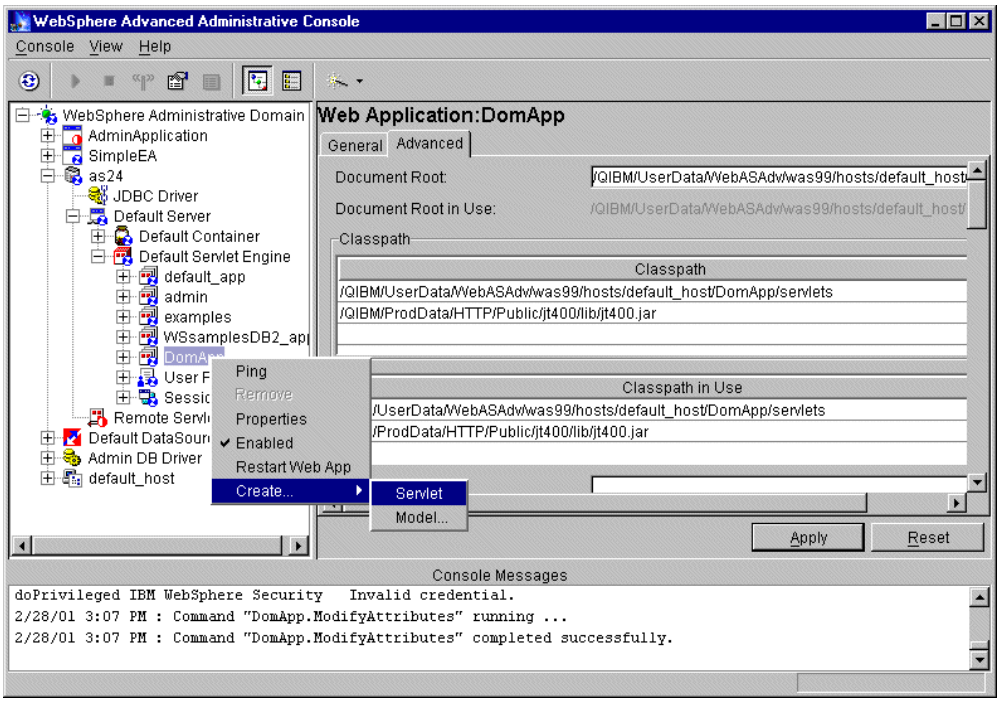

Figure 27. Web application: Create servlet

__ 22. In the Create Servlet window shown in Figure 28, enter the following values:

- Servlet name: `SimpleServlet`
- Web Application: `DomApp`
- Description: `SimpleServlet example for Single Sign-On`
- Servlet Class Name: `SimpleServlet`

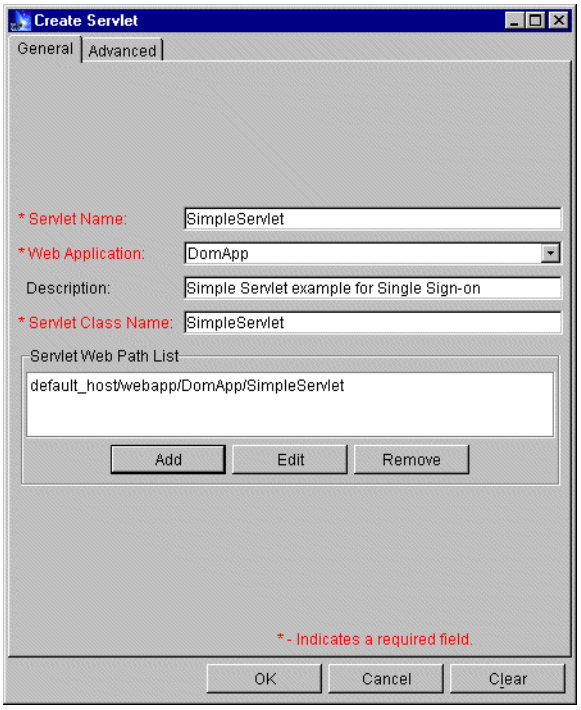

Figure 28. Create Servlet

- Servlet Web Path List: Add the following path by clicking on the **Add** button and appending the name **SimpleServlet** to the predefined servlet path as shown in Figure 29:

  `default_host/webapp/DomApp/SimpleServlet`

  Click **OK**.

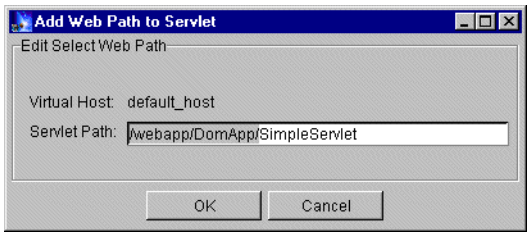

Figure 29. Add Web Path to Servlet

__ 23. Back in the *Create Servlet* dialog (Figure 28), click **OK**.

__ 24. After a couple of seconds (or possibly longer), a dialog box indicating that the servlet was created successfully appears. Click **OK** (Figure 30).

Figure 30. Servlet created successfully

__ 25. Restart the Web Application so your changes take effect. Right-click **DomApp**, and select **Restart Web App** (Figure 31).

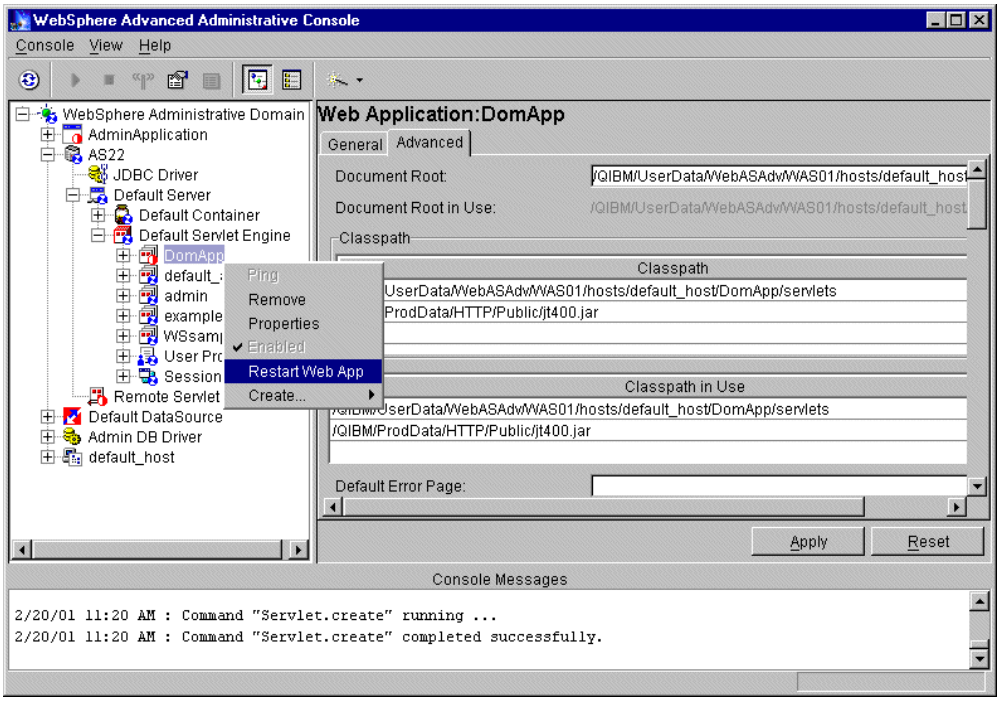

Figure 31. Restart Web application

__ 26. If the Web application (DomApp) starts successfully, the successful completion dialog box appears (Figure 32). The SimpleServlet icon should be blue. You should see it when you expand the tree under DomApp.

Figure 32. Restart DomApp successful

__ 27. You can now test the SimpleServlet using the Ping command. Right-click **SimpleServlet** and then select **Ping** (Figure 33).

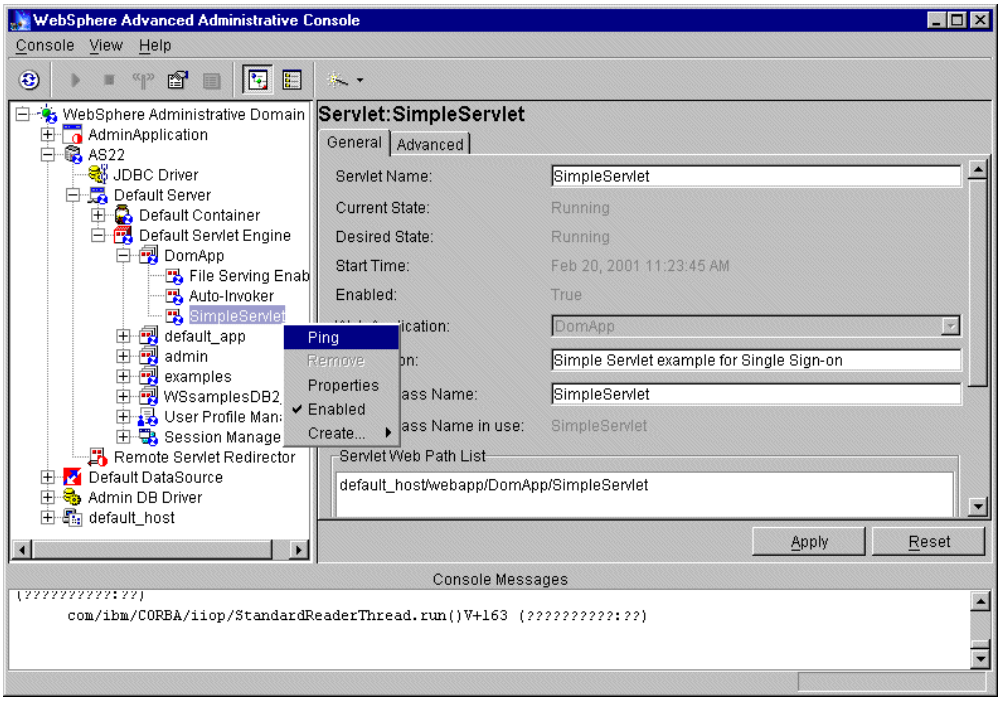

Figure 33. Ping SimpleServlet

If everything is successful, you should see the dialog box shown in Figure 34. This means the WebSphere configuration is correct, but it does *not* mean that the servlet is valid. You need to run the servlet to verify it.

Figure 34. SimpleServlet.ping successful message

Task 5: Testing SimpleServlet

Now that your servlet is available through WebSphere Application Server 3.5.2, you can test it by opening the URL through a Web browser.

__ 1. To run the servlet outside of the WebSphere Administrative Console, open your Netscape browser and enter the following URL:

```
http://PWDI.PID.IBM.COM:80xx/webapp/DomApp/SimpleServlet
```

__ 2. You are prompted to accept a cookie (Figure 35). Click **OK**.

Figure 35. Cookie

You should see the Web page shown in Figure 36.

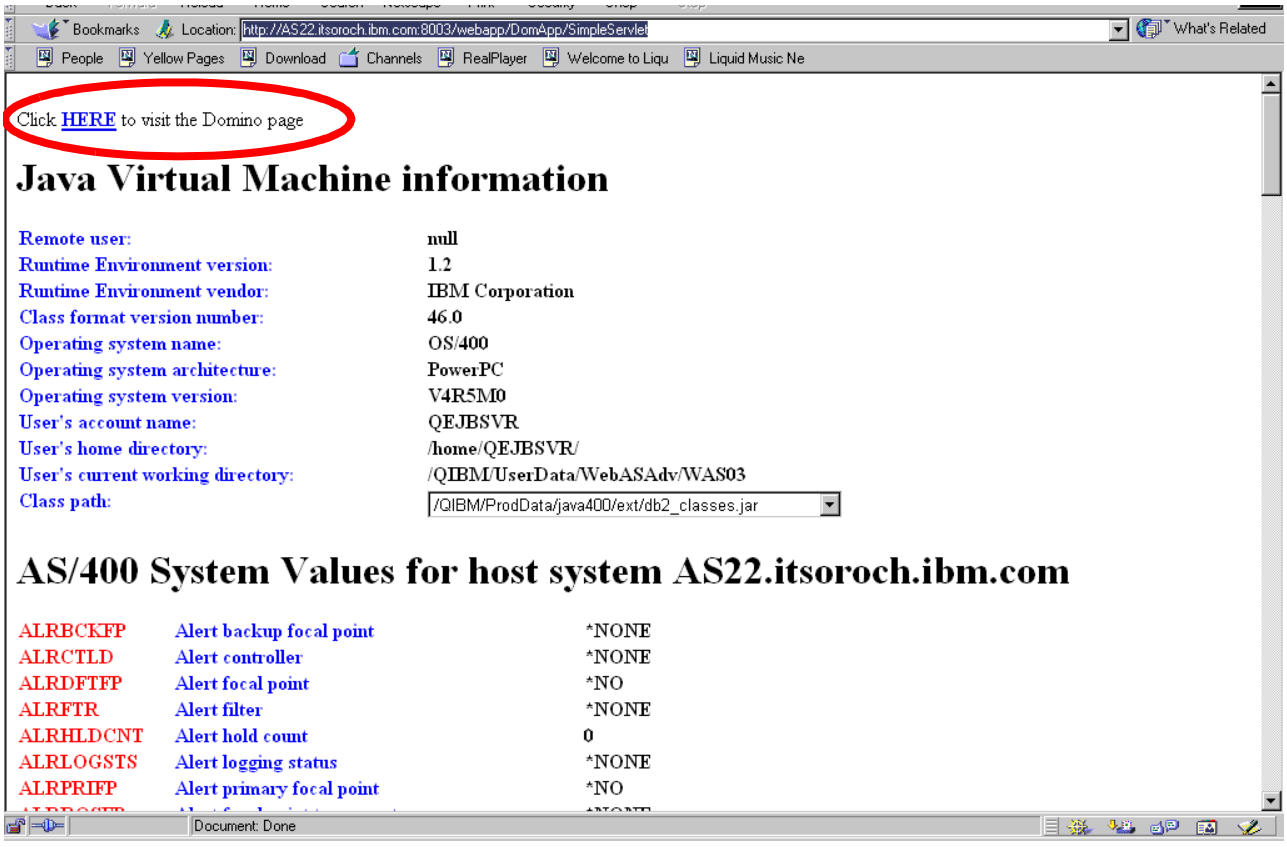

Figure 36. SimpleServlet accessed via a Web browser

__ 3. To access the Domino application from the servlet, click the link:

```
Click HERE to visit the Domino page
```

You should see the Domino application shown in Figure 37. Remember, at this point you have not configured any security for either Domino or WebSphere. That is your next task.

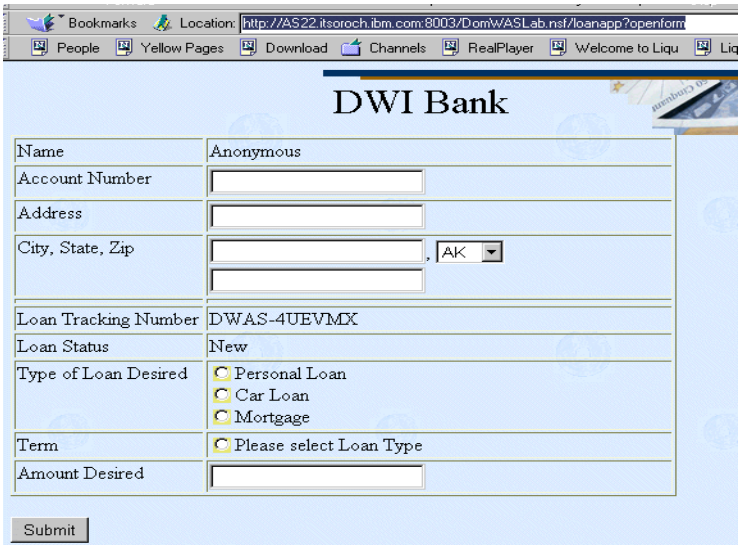

Figure 37. Domino application

__ 4. Close the Netscape browser window.

Lab 3. Enabling Domino authentication

In the previous labs, you used the HTTP server of Lotus Domino for AS/400 without enabling authentication, because you did not change the default authority for anonymous users on the Domino application database (DomWASLab.nsf). This will be the focus of this lab.

Objectives

This lab teaches you how to prevent Web browsers from opening a Domino database without specifying a valid user ID and password.

Important

Throughout these lab exercises, replace *xx* with your team number and refer to Table 1 on page 4 to make sure the correct values for the configuration parameters are entered.

Task 1: Securing your Domino database

In this task, you secure the Domino database (DomWASLab.nsf) you created in Lab 1. “Developing a Domino application” on page 9, by defining an access level of “none” for anonymous users.

__ 1. Open the Domino Administrator client by clicking on the icon on your desktop, or select **Programs->Lotus Applications->Lotus Domino Administrator** from the Start menu. The password for the user Notes Guru/Domxx is `dom2was`.

__ 2. Make sure that the Domino Administrator client is pointing to *your* Domino server (DOMWASxx/Domxx). If the upper left of the screen reads Server:Local, you should select **File->Open Server** from the menu bar and select **DOMWASxx/Domxx**.

__ 3. From the Files tab, right-click the **DomWASLab.nsf** database and select **Access Control->Manage** to open the ACL of the database.

__ 4. Click **Add** and type `Anonymous` into the “Person, server or group” field and click **OK**.

__ 5. For Access, select **No Access**. Deselect **Read public documents** and **Write public documents**. Click **OK**.

__ 6. Minimize the Domino Administrator client.

Note: You can also achieve the same result from a Notes Client by opening the DomWASLab.nsf database on the DOMWASxx server and select **File->Database->Access Control**.

Task 2: Experiencing the Domino security challenge

You now need to test your changes by accessing the Domino application again from a Web browser. This time you are challenged to enter a username and password just before the loan application form opens. This is a challenge from

Domino (we have not yet turned on security in WebSphere). Since you have closed down Anonymous access to the database, Domino now needs to know who you are.

__ 1. From the Netscape browser, test the Domino Web application (DomWASLab.nsf) by entering the following URL (remember to replace *xx* with your team number):

```
http://PWDI.PID.IBM.COM:80xx/DomWASLab.nsf/loanapp?openform
```

__ 2. The window shown in Figure 38 appears and prompts you for a valid User Name and Password. Enter the user name `Notes Guru`, and password `dom2was`. Click **OK**.

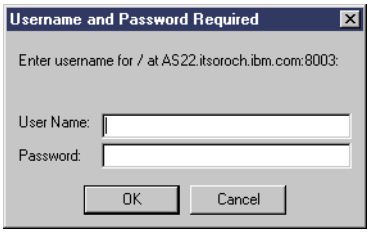

Figure 38. Domino challenge to access DomWASLab.nsf

__ 3. Also notice that, on the loan application, the name field is filled in with your name (Notes Guru) because Domino now knows who you are. However, WebSphere still doesn't know or require your identity.

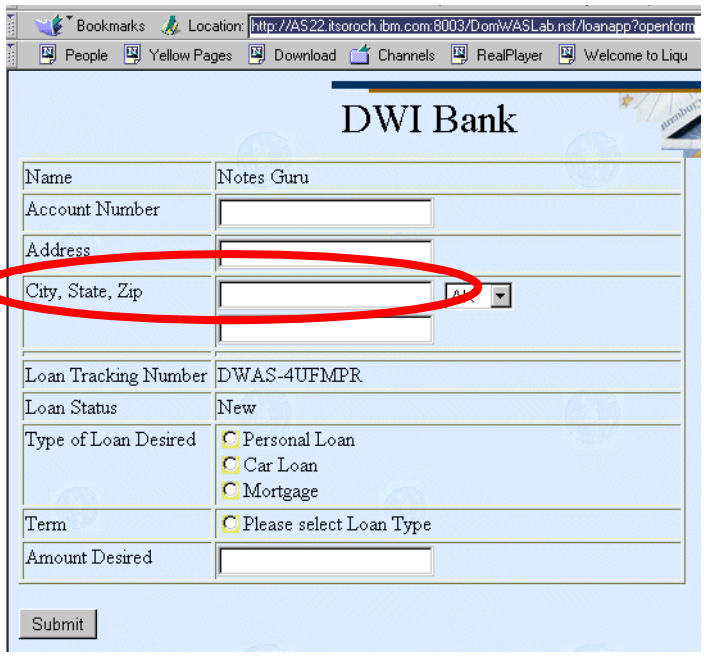

Figure 39. Domino loan application with Name field filled in automatically

__ 4. Click **Submit** to proceed to the link to the WebSphere SimpleServlet.

__ 5. On the next Web page that is displayed (Figure 40) click the **Return to the Main Menu** link to proceed to the WebSphere SimpleServlet.

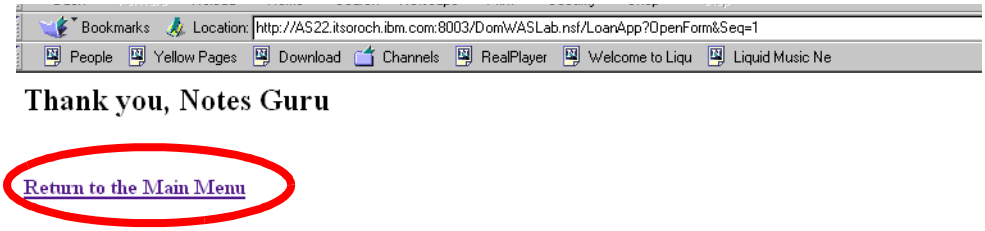

Figure 40. Domino application link to SimpleServlet

__ 6. You are prompted to accept a cookie (Figure 41). Click **OK**.

Figure 41. Cookie

You should see the Web page shown in Figure 42.

__ 7. Because you have not yet enabled WebSphere authentication, you immediately see the WebSphere SimpleServlet (Figure 42).

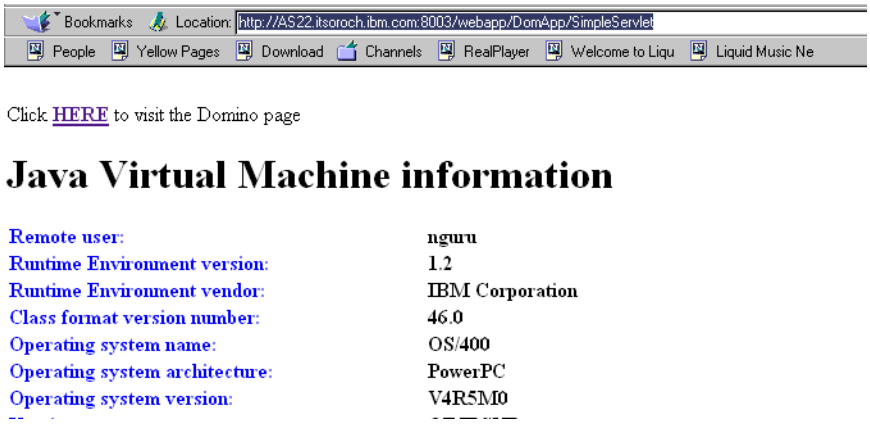

Figure 42. WebSphere SimpleServlet

__ 8. Close the Netscape browser window.

Lab 4. Enabling WebSphere authentication

Similar to Domino, WebSphere Application Server 3.5.2 does not by default require users to enter a user name and password to access any of the resources it manages. Several steps need to be performed to activate security. With WebSphere Application Server, you can secure your applications by configuring the following security policies:

- Authentication: Determination of who is making a request
- Authorization: Determination of whether a request is to be honored
- Delegation: Determination of who will be handling the request

In this lab, you enable authentication for your instance of WebSphere Application Server 3.5.2. You then define the authorization to access the Web application (DomApp) created in Lab 2. “Creating a simple Web application” on page 17.

Objectives

This lab teaches you how to:

- Configure Domino as an LDAP server.
- Enable security for the WebSphere Application Server 3.5.2.
- Protect WebSphere components of a Web Application.

Important

Throughout these lab exercises, replace *xx* with your team number and refer to Table 1 on page 4 to make sure the correct values for the configuration parameters are entered.

Task 1: Configuring Domino as an LDAP server

Domino R5 supports access to the Domino directory via LDAP. If you configured the Domino server with the Directory Services parameter set to LDAP, no further action is required since the configuration automatically changes the Domino Server configuration document and adds LDAP to the Server Tasks line in the notes.ini file.

For this lab, your Domino server has not been automatically configured with LDAP because, by default, LDAP servers listen on port 389, which conflicts with the other student Domino servers and with the OS/400 LDAP server.

In this lab, the LDAP port number needs to be changed to listen on a different port. The only steps necessary for enabling LDAP access to the Domino Directory are to change the LDAP port in the Domino Server configuration document and start or re-start the Domino LDAP server task.

To change the LDAP port on a Domino server, perform the following steps:

__ 1. Start the Domino R5 Administrator client.

__ 2. Open your Domino server and select the **Configuration** tab.

__ 3. Select **Server->Current Server Document view** to display the Domino Server document.

__ 4. Click the **Edit Server** button.

__ 5. Click the **Ports** tab.

__ 6. Click the **Internet Ports** and **Directory** sub-tabs to display the LDAP port settings (see Figure 43).

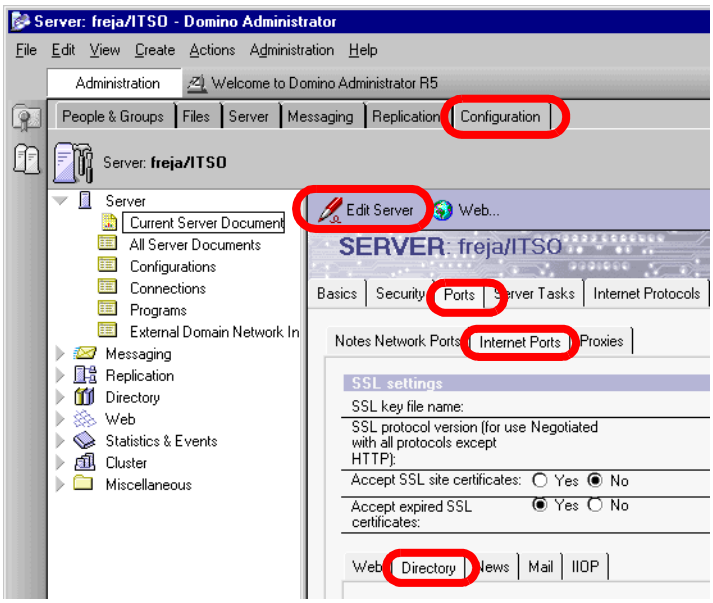

Figure 43. Domino Administrator client showing Internet port settings

Recommendation

We recommend that, for a production environment, the TCP/IP port be disabled and the SSL port be enabled with at least “Name & password” authentication. Hoever, do not enable the SSL port during this hands-on lab!

__ 7. The default LDAP standard and SSL port numbers (389 and 636) are shown. Ensure that the TCP/IP port status is set to `Enabled`, and change the port number to `389xx` as shown in Figure 44.

Click **Save and Close** to save your change.

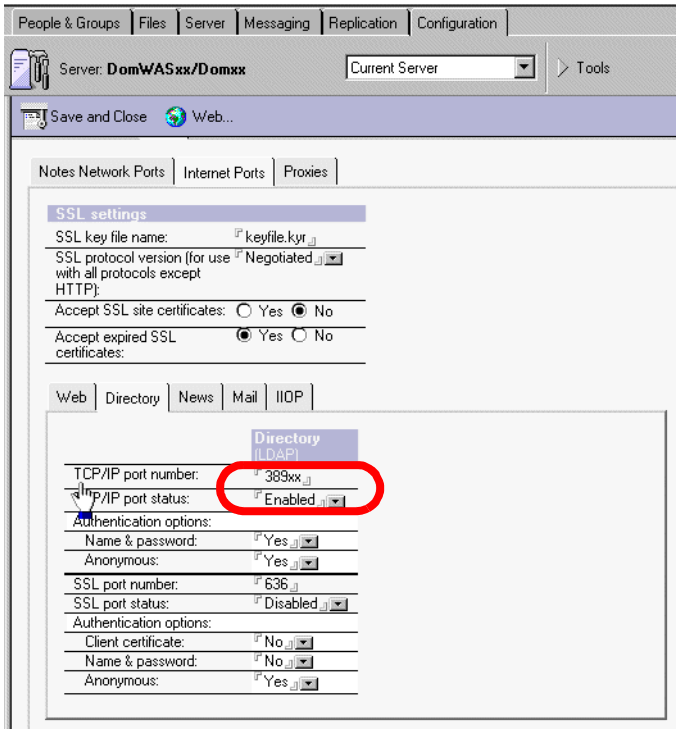

Figure 44. LDAP port settings for the Domino directory

__ 8. You now need to start the LDAP server task on your Domino server. Click the **Server** tab and then the **Status** sub-tab. Now click on the **Task** button on the right side of window and click **Start** (Figure 45).

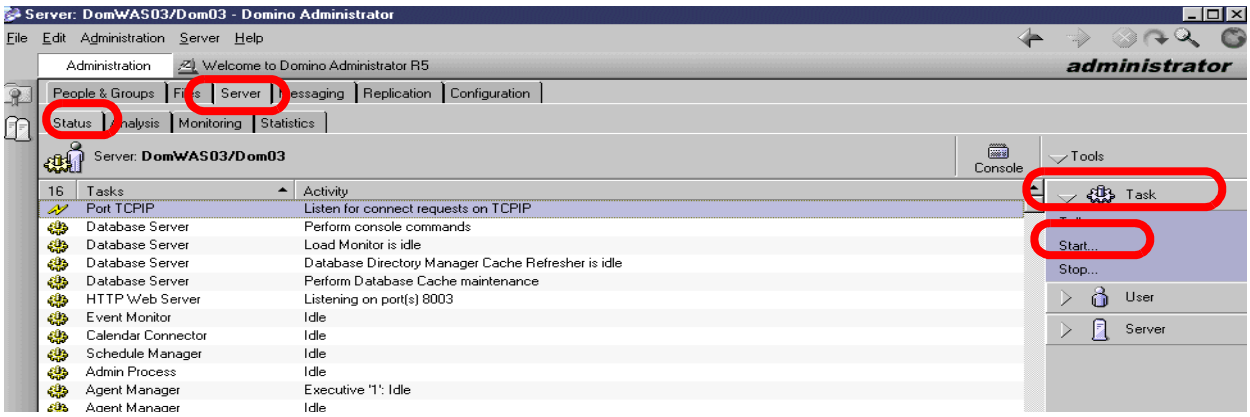

Figure 45. Domino server status view

__ 9. From the Start New Task window, scroll down and select the **LDAP Server** task, and click the **Start Task** button to start the LDAP server. See **Figure 46**.

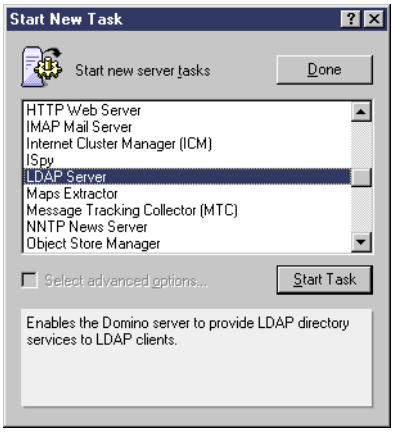

Figure 46. Start LDAP server task

__ 10. Click **Done** to close the dialog window.

__ 11. Minimize the Domino Administrator.

Tip

The LDAP server task can also be started from the Domino console by entering the `Load LDAP` command. You can also add the LDAP server task to the Server Tasks line in the Domino server's NOTES.INI file to start the task automatically each time the Domino server is started. If you picked LDAP support during the configuration of the Domino server, this entry is already in the NOTES.INI file.

Task 2: Enabling security for the WebSphere Application Server 3.5.2

To restrict the use of WebSphere Application Server 3.5.2 by allowing only *authenticated users* access to its resources, a user registry (a directory of valid users) needs to be in place. This can either be the user registry provided by the platform on which WebSphere is running (for OS/400 this would be the user profiles), or any LDAP server. On an iSeries 400 or AS/400 server, an LDAP server can be either SecureWay Directory for OS/400 or Lotus Domino for AS/400.

If you plan to use the same user registry for multiple servers and later enable Single Sign-On (which you do in this lab), you *must* use an LDAP server for authentication.

During the next labs, you use Lotus Domino for AS/400 as your LDAP server. Later, in Lab 6. “Optional lab: Using the OS/400 LDAP server” on page 91, you have the option to change the configuration to use SecureWay Directory for OS/400.

Ensuring that the LDAP task in Domino is running

Because several students are using their partitioned Lotus Domino for AS/400 server, you needed to modify the port number your LDAP server is running on. At this point, it is a good idea to verify that the LDAP task of your Domino server is running and listening to the correct 389xx port number (remember that *xx* is you team number).

__ 1. On your Windows Desktop, double-click the icon for the 5250 emulation session.

__ 2. Sign on to the classroom AS/400 or iSeries server, PWDI (user `DOMWASxx` and password `dom2was`).

__ 3. Type the following command on the OS/400 command line and press Enter:

```
WRKDOMSVR DOMWASxx
```

__ 4. Type option `8` (Work with console) in the Opt field next to *your* Domino server (DOMWASxx). Make sure you select the correct Domino server, with *xx* being your team number. Press Enter.

__ 5. In the command line at the bottom of the *Work with Domino Console* panel, enter either the `sh ta` command, or its long form (`show tasks`), and press Enter.

__ 6. Scroll down until a panel similar to the one shown in Figure 47 appears.

```
                        Work with Domino Console
                                                    Server: DOMWASxx
Previous subcommands and messages:
   Schedule Manager     Idle
   Admin Process        Idle
   Agent Manager        Executive '1': Idle
   Agent Manager        Idle
   Stats                Idle
   Indexer              Idle
   Router               Idle
   Replicator           Idle
   Billing              Idle
   HTTP Web Server      Listening on port(s) 80xx
   LDAP Server          Listen for connect requests on TCP Port:389xx
   LDAP Server          Control task
   DECS Server          Idle


Enter a Domino subcommand.
===> ____________________________________________________________________

F3=Exit    F5=Refresh    F6=Print    F9=Retrieve
F17=Top    F18=Bottom    F21=Command line
```

Figure 47. Work with Domino Console: Show tasks command

__ 7. Make sure the LDAP Server is actually listening to the LDAP port assigned to your team (389xx). If it is not, go back to the previous steps and try to determine your problem.

__ 8. Press F3 to exit the Domino console.

Checking the connection to LDAP

Perform the following tasks to check your connection to LDAP:

__ 1. To actually check your connection to your Domino LDAP server, enter the following command on the OS/400 command line and press Enter:

```
qsh
```

__ 2. Enter the following Qshell command:

```
ldapsearch -h DOMWASxx -p 389xx objectclass=*
```

A listing of your Domino Directory in LDAP format should appear. If you recieve an error message, that command ldapsearch cannot be found, try to sign off and sign on again.

Setting up WebSphere Application Server 3.5.2 Global Security

You can now set up WebSphere to authenticate users before giving them access to resources.

__ 1. If it is not already started, start the WebSphere administrative console and connect it to your WebSphere instance. To do this, bring up a DOS prompt on your local machine and enter the following commands:

```
C:>cd \WebSphere\Appserver\bin    <Press Enter>
C:\WebSphere\Appserver\bin\>adminclient PWDI 9xx    <Press Enter>
```

Be sure to type the host name (PWDI) in upper case and use the correct port (9xx).

__ 2. The console takes some time to start, and you may see the *Establish Connection* or *Loading ...* panel for several seconds or even minutes.

__ 3. In the WebSphere Administrative Console, click the **Wizards** button.

__ 4. Select **Configure Global Security Settings** to start configuring security for the administrative domain as shown in Figure 48.

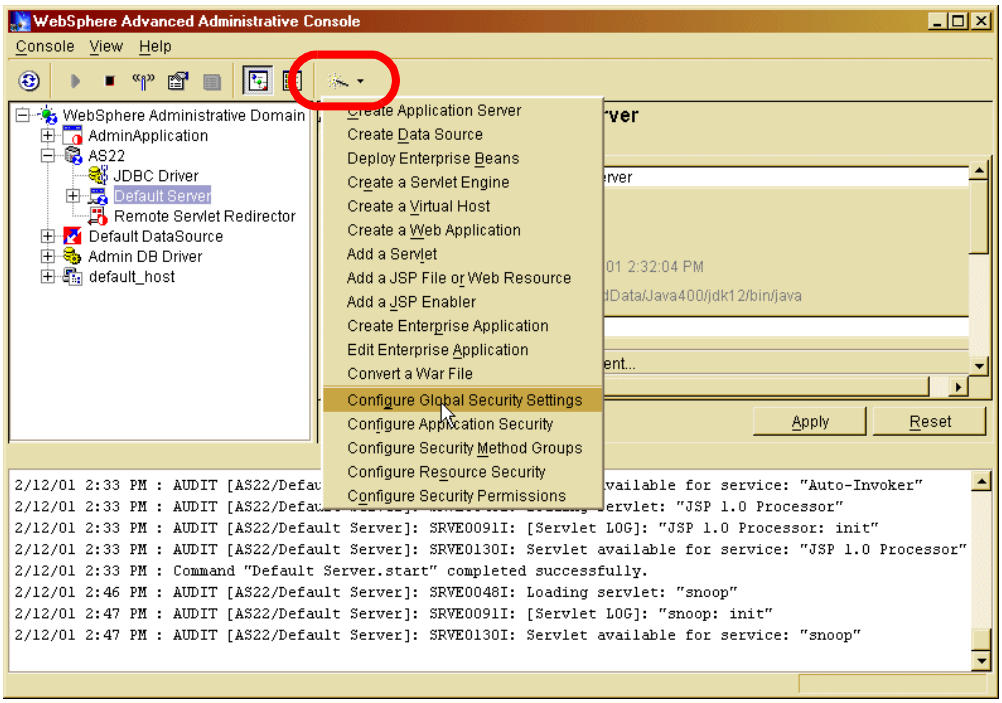

Figure 48. Configure WebSphere Global Security Settings

5. The *Set Global Security Wizard* opens with the General tab already selected as shown in Figure 49.

   a. Select the **Enable Security** checkbox to enable security.

   b. Verify that the Security Cache Timeout is set to a reasonable value. When the timeout is reached, WebSphere Application Server clears the security cache and rebuilds the security data. If the value is set too low, the extra processing overhead may be unacceptable. If the value is set too high, you create a security risk by caching security data for a long period of time. The default value is 600 seconds.

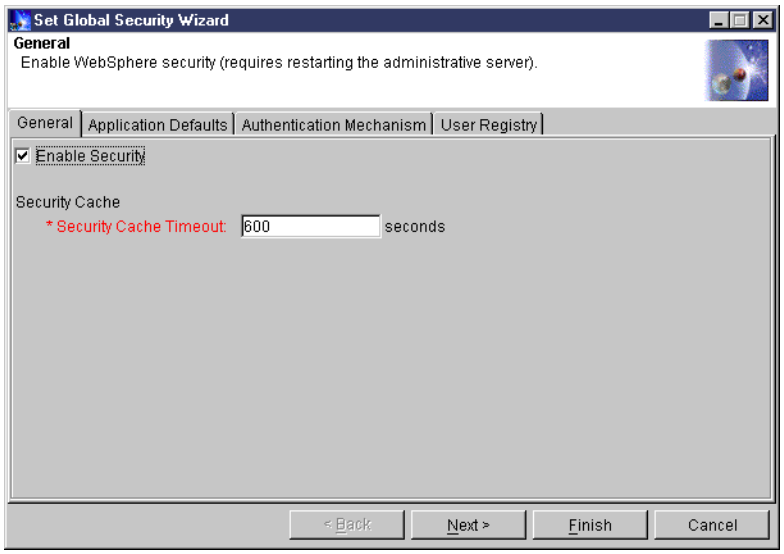

Figure 49. Set Global Security Wizard: General tab

__ 6. Click the **Application Defaults** tab or the **Next >** button.

   a. Set Realm Name to the domain portion of your fully qualified Internet name for the system running your WebSphere administrative domain (see Figure 50). For this lab, use `PID.IBM.COM` for this field.

   b. Select **Basic (User ID and Password)** for the Challenge Type.

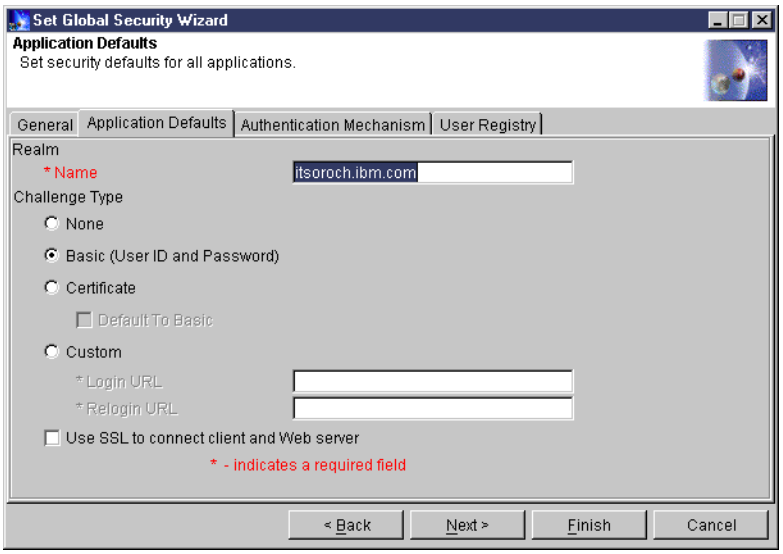

Figure 50. Set Global Security Wizard: Application Defaults tab

__ 7. Click the **Authentication Mechanism** tab or the **Next >** button. In the window that appears (Figure 51), enter the following information:

a. Set Authentication Mechanism to **Lightweight Third Party Authentication (LTPA)** to use an LDAP directory as the user registry.

b. At this point, *do not* click the Enable Single Sign-On (SSO) box. For this lab, you should first experience how authentication works *without* using Single Sign-On.

c. You cannot enter a Domain unless you enable Single Sign-On. Because you do not enable SSO until the next lab, leave this field blank.

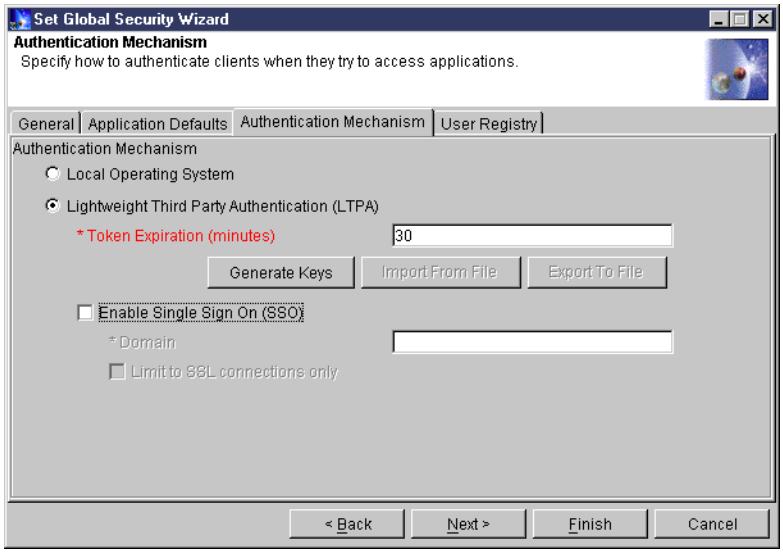

Figure 51. Set Global Security Wizard: Authentication Mechanism tab

__ 8. Click the **User Registry** tab or the **Next >** button. To enable Single Sign-On (which is your ultimate goal), the user registry must be an LDAP directory managed by an LDAP server that is currently running. The wizard attempts

to connect to the LDAP server to verify the information you enter. Fill in the LDAP fields as explained in the following list (see Figure 52):

- **Security Server ID** = **nguru**

  This is the user ID of the administrator for the WebSphere administrative domain. This user ID is used later when accessing WebSphere administration services using the WebSphere Administrative Console. By default, this should be the value of the short name or user ID for a user already defined in the LDAP directory. Do not specify a Distinguished Name by using *cn=* or *uid=* before the value.

  Note: Later, when you start the WebSphere Administrative Console, you must enter the value exactly as you specified it in this field.

- **Security Server Password** = **dom2was**

  This is the valid password for the Security Server ID. This field is case-sensitive.

- **Directory Type = Domino 5.0**

  This value should be set for the type of LDAP server you are using. For example, select SecureWay for IBM SecureWay LDAP Directory, or Domino 5.0 for Domino LDAP directory.

- **Host = DOMWASxx.PID.IBM.COM** (*xx* = team number)

  This is the fully qualified host name on which the LDAP directory is running.

- **Port = 389xx** (*xx* = team number)

  This is the port on which the LDAP directory runs. You may leave this field blank for the default non-SSL (secure sockets layer) port of the LDAP directory (port 389).

- **Base Distinguished Name = <leave this field blank>**

  This is the Distinguished Name (DN) of the directory in which searches begin within the LDAP directory. For example, for a user with a DN of cn=John Doe, ou=Rochester, o=IBM, and c=US, you could specify a base DN of ou=Rochester, o=IBM, c=US or o=IBM, c=us or c=us. This is a required field for all LDAP directories except the Domino Directory.

  Note: If you are using the Domino Directory, and you specify a Base Distinguished Name, you can not grant permissions to individual Web users for resources managed by your WebSphere application server.

- **Bind Distinguished Name = <leave this field blank>**

  This is the DN of the user who is capable of performing searches on the directory. In most cases, this field is not required since all users are usually authorized to search an LDAP directory. However, if the LDAP directory contents are protected from all LDAP users, you need to specify the DN of an authorized user, such as the administrator of the directory (for example, cn=Administrator).

- **Bind Password = <leave this field blank>**

  This is the valid password for the user specified as the Bind Distinguished Name. This is required only if you specify a value for Bind Distinguished Name. This field is case-sensitive.

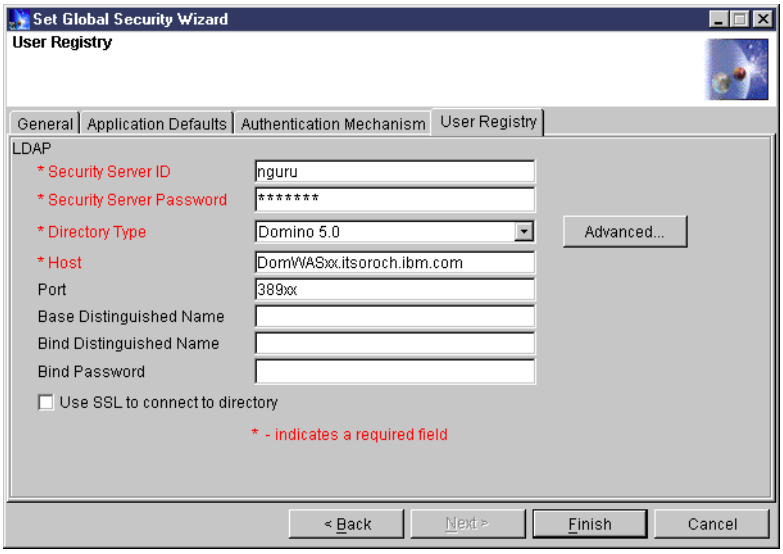

Figure 52. Set Global Security Wizard: User Registry tab

__ 9. Click **Finish** to save the Global Security Settings.

__ 10. The LTPA Password window appears (Figure 53). This is the password for the keys that WebSphere is generating. For this lab, enter `dom2was`. Click **OK**.

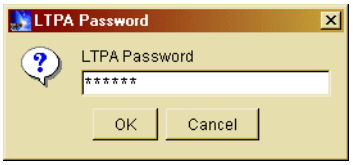

Figure 53. LTPA Password for generation of keys

__ 11. After a couple of seconds, a message box appears (Figure 54) stating that your changes will not take effect until the WebSphere Administrative server is restarted. Click **OK** to continue.

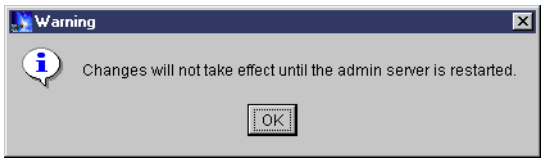

Figure 54. Global Security Settings finished successfully message

__ 12. To restart the WebSphere Administrative server, right-click on the node (PWDI) and select **Restart** (Figure 55). Be patient, the context menu may not appear immediately.

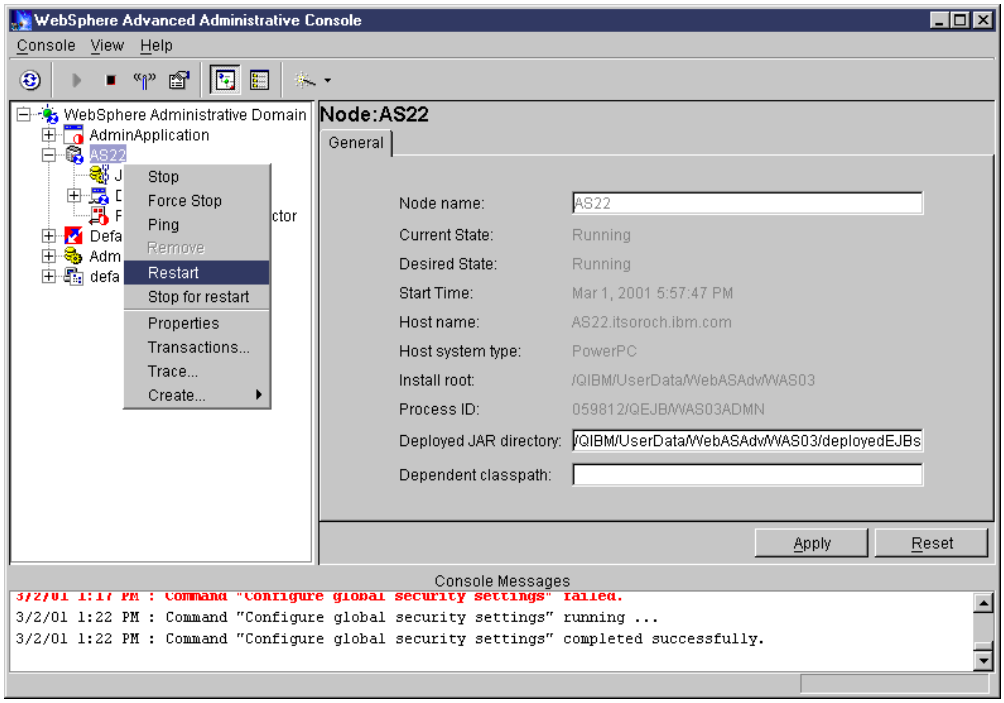

Figure 55. Restarting the WebSphere server

__ 13.A warning message appears (Figure 56) stating that you are trying to stop the node to which the console is connected. Click **Yes** to continue.

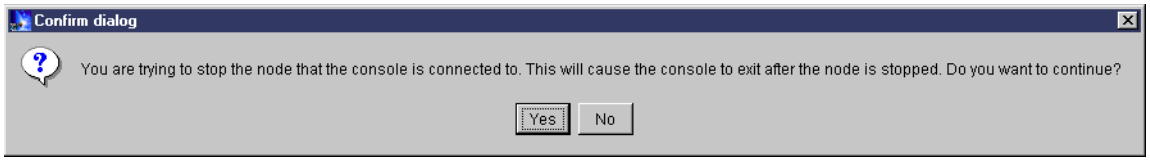

Figure 56. Restart WebSphere warning message

__ 14.Make sure that your WebSphere monitor job (WASxxMNTR) and the administrative server job (WASxxADMN) for your team is completely restarted before continuing with the lab. To check this, perform the following tasks:

a. Enter the Work with Active Jobs (WRKACTJOB) command to verify that they are in JVAW and EVTW status:

```
wrkactjob sbs(qejbsbs)
```

Monitor the administrative server task (or job) (WASxxADMN) from the Work with Active Jobs screen (WRKACTJOB) to ensure that the WebSphere Administrative server restarts successfully. As you watch the Administrative server job, notice that it stops, starts, stops, and then starts again. This is expected after Global Security Settings have been changed.

b. Display the joblog for the administrative server job (WASxxADMN). From the WRKACTJOB display, enter option `5` (Work with) next to the WASxxADMN job. Press Enter. Note, it may take several minutes - possibly more than ten minutes - depending on how busy the system with all students' work is. (Probably a good time for a coffee break.)

3. On the Work with Job display, enter option `10` (Display job log, if active or on job queue) to display the joblog. Press Enter.

d. Look for the following message:

```
WebSphere administration server WASxxADMN ready.
```

You may have to press F5 several times to refresh the display and scroll down if you see **More...** in the lower right corner of your display.

e. Position the cursor on the ready message (step d). Press F1 to verify that the administration server is listening to the correct port assigned to your team (9xx) and that the message is new (look at the time stamp). See Figure 57.

```
                    Additional Message Information

Message ID . . . . . :   EJB0106      Severity . . . . . :   00
Message type . . . . . :   Information
Date sent  . . . . . :   02/18/01     Time sent  . . . . . :   11:13:53

Message . . . . :   WebSphere administration server WASxxADMN ready.
Cause . . . . . :   WebSphere administration server WASxxADMN is ready to
  handle requests from the WebSphere administration console on port 9xx.
  Diagnostic information is controlled on port 20834.
```

Figure 57. WebSphere administration server started successfully

__ 15. Once the WebSphere Administrative Server has been successfully and completely restarted, restart the WebSphere administrative console and connect it to your WebSphere instance. To do this, bring up a DOS prompt on your PC client and enter the following commands:

```
C:\>cd \WebSphere\Appserver\bin      <Press Enter>
C:\WebSphere\Appserver\bin\>adminclient PWDI 9xx      <Press Enter>
```

Be sure to type the host name (PWDI) in upper case and use the correct administrator server port (9xx).

__ 16. You now need to sign on to the WebSphere Administrative console because you enabled security. Specify the user ID and password exactly as you configured previously for the Security Server ID and Security Server Password fields in the Global Security Settings wizard (Figure 58).

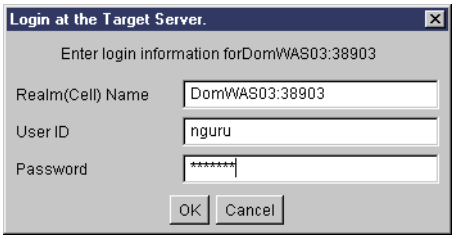

Figure 58. Sign on to the WebSphere Administration Console

__ 17. Wait until the WebSphere Administrative message console displays the *Console Ready* message before continuing with the next task.

Task 3: Protecting WebSphere components of the sample Web application

After activating Global Security for your WebSphere Application Server 3.5.2, you need to protect your resources. This is called “creating an authorization policy”, and is performed from the WebSphere Administrative Console. For the example used in this lab, the five following steps are performed:

1. “Creating an Enterprise Application” on page 59
2. “Configuring Application Security” on page 61
3. “Configuring Resource Security” on page 64
4. “Configuring Security Permissions” on page 66
5. “Starting SimpleEA” on page 70

The following sections describe these steps in detail.

Creating an Enterprise Application

In this lab so far, you have made a servlet available through the WebSphere Application Server 3.5.2 and configured Global Security. To protect any resources managed by WebSphere, an Enterprise Application needs to be created.

An Enterprise Application is a collection of resources that can be protected as a whole. It is usually comprised of enterprise beans, servlets, Java ServerPages, and other resources that perform an aspect of business logic.

__ 1. Click the **Wizard** icon as shown in Figure 59, and select **Create Enterprise Application**. Or, from the WebSphere Administrative Console pull-down menu, select **Console->Tasks->Create Enterprise Application**.

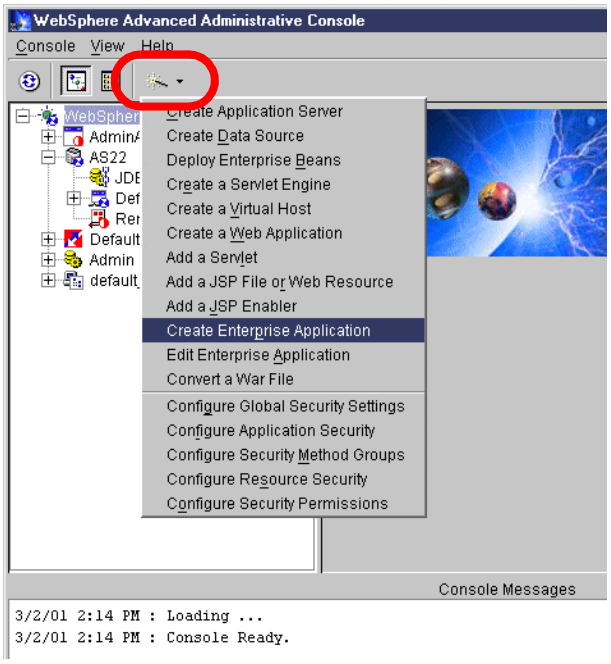

Figure 59. Create Enterprise Application

__ 2. In the Application Details window (Figure 60), enter the name for the new Enterprise Application (`SimpleEA`). Click **Next>** to continue. Make sure not click the Next> button twice. It may take more than 4 minutes until the next

panel appears. Also the busy icon (hourglass) will not appear unless you move the cursor off the *Create Enterprise Application Wizard* window.

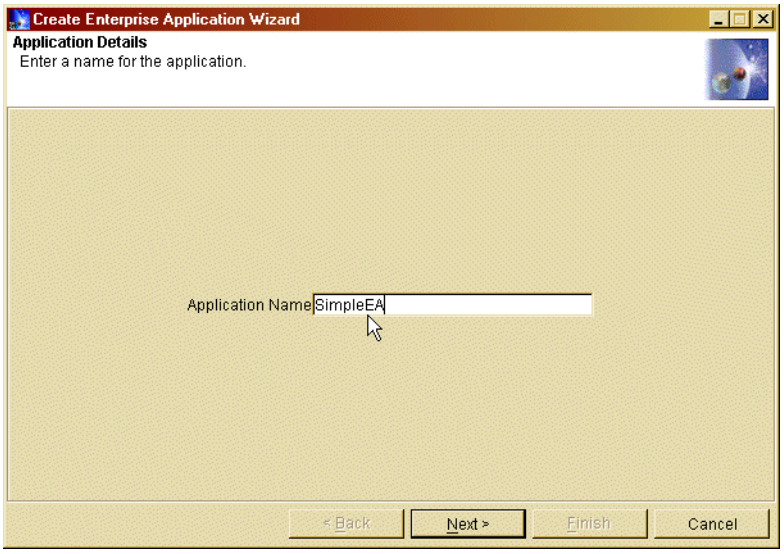

Figure 60. Create Enterprise Application Wizard: Application Details

__ 3. After several minutes, the Application Resources window (Figure 61) appears. Once you see it, click the plus (**+**) sign next to Web Applications to expand the tree underneath it. It will also take two or three minutes to expand the tree.

__ 4. Select your **DomApp** Web application, and click the **Add** button.

__ 5. Click the **Next>** button.

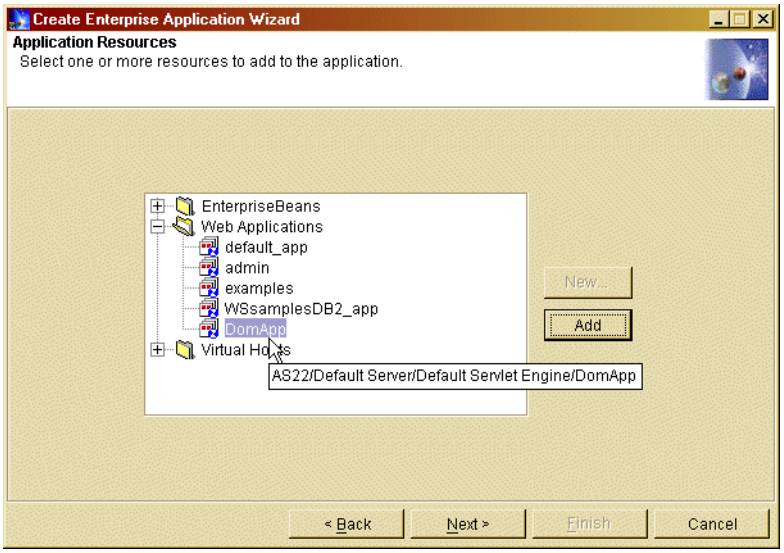

Figure 61. Create Enterprise Application Wizard: Application Resources

__ 6. You now see another Application Resources window (Figure 62). This allows you to remove unwanted Web applications from your new Enterprise

Application. Click the plus (**+**) sign to expand Web Applications and ensure DomApp was added. Click **Finish**.

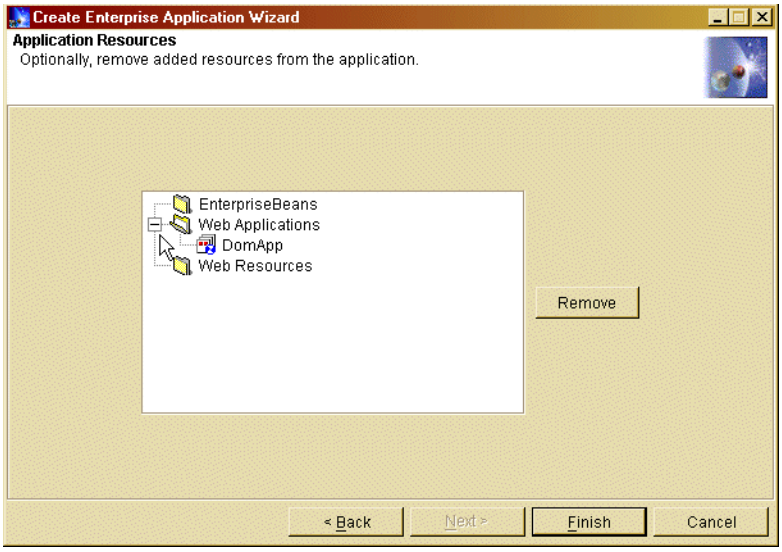

Figure 62. Create Enterprise Application Wizard: Application Resources - Remove resources

__ 7. It may take a few of minutes to create the Enterprise Application. Wait until the confirmation window is shown (Figure 63). Click **OK**.

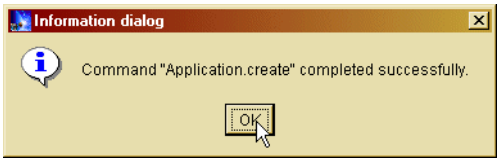

Figure 63. Enterprise Application created successfully message

A new Enterprise Application (SimpleEA) has now been created within your WebSphere Application Server 3.5.2.

Configuring Application Security

In this section, you enable security for your Enterprise Application.

__ 1. Click the **Wizard** icon and select **Configure Application Security** as shown in Figure 64.

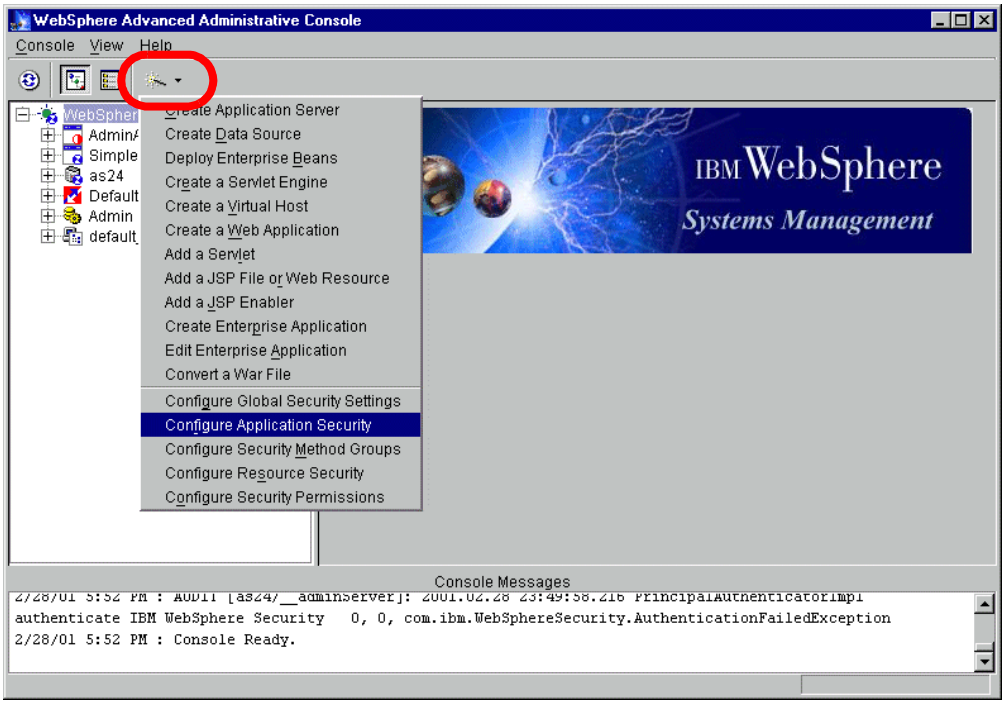

Figure 64. Configure Application Security

__ 2. On the Enterprise Applications window, click the plus (**+**) sign next to Enterprise Applications to expand the tree. Click **SimpleEA**, and then click **Next>** (Figure 65).

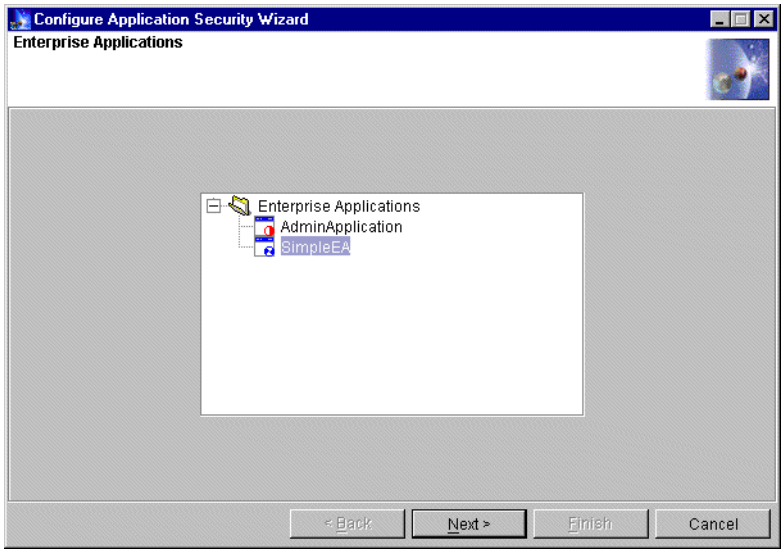

Figure 65. Configure Application Security Wizard: Enterprise Applications

__ 3. On the Realm and Challenge Type window, ensure that the realm name is `PID.IBM.COM` and the challenge type is `Basic (User ID and Password)`. Leave the rest of the options as the defaults, and click **Next>** (Figure 66).

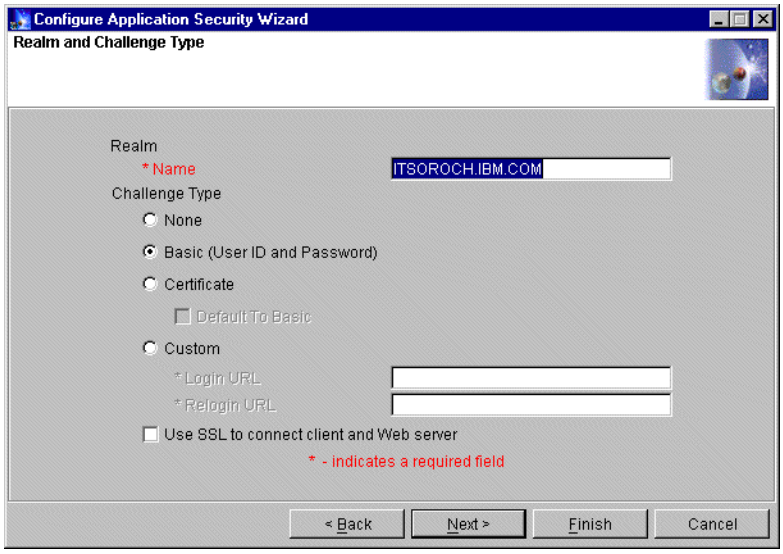

Figure 66. Configure Application Security Wizard: Changing Realm and Challenge Type

__ 4. Leave the Application Identity screen default, and click **Finish** (Figure 67).

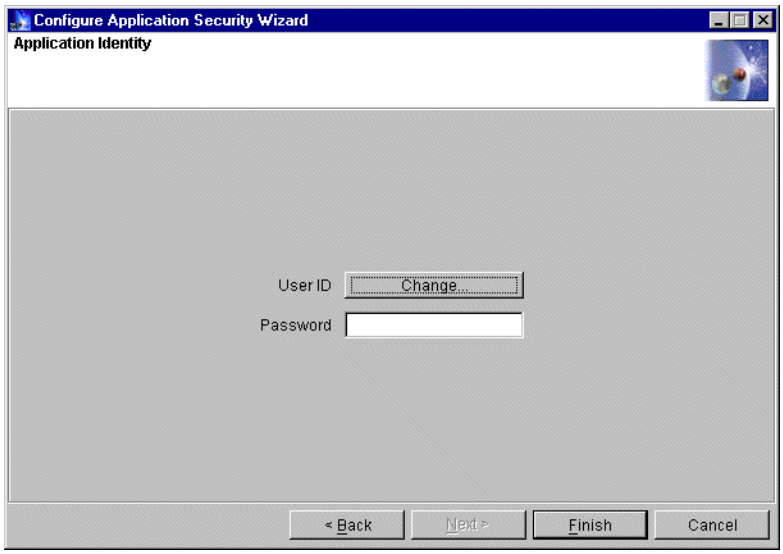

Figure 67. Configure Application Security Wizard: Application Identity

__ 5. After the console message appears stating that Application Security was configured successfully (Figure 68), you can continue to the next step.

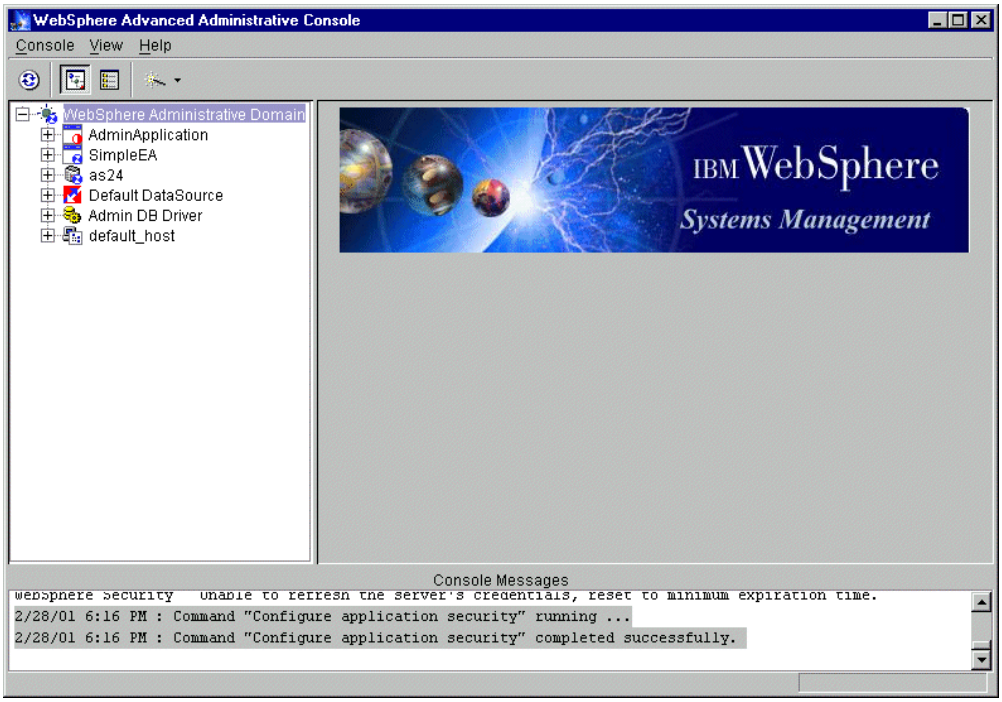

Figure 68. Application Security configured successfully

Configuring Resource Security

To enable security for the Enterprise Application, you must configure Resource Security. This sets security for the components of the Enterprise Application.

__ 1. Click the **Wizard** icon, and select **Configure Resource Security** as shown in Figure 69.

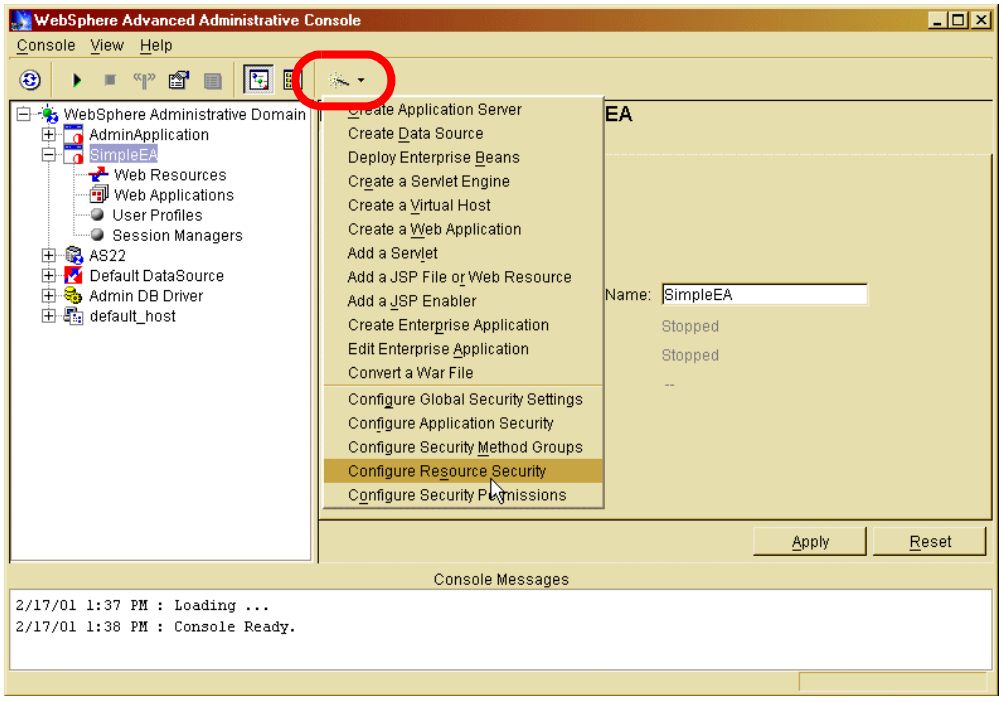

Figure 69. Configure Resource Security

__ 2. Once it appears, expand the *Virtual Hosts* tree by clicking the plus (**+**) sign next to Virtual Hosts.

Note: Be patient and click the plus sign only once because it takes a few minutes until the the tree expands. When you perform this step the first time, the mouse pointer may not change to an hour glass.

__ 3. Expand the *default_host* tree. Again, it may also take a while to expand the tree for the very first time (Figure 70).

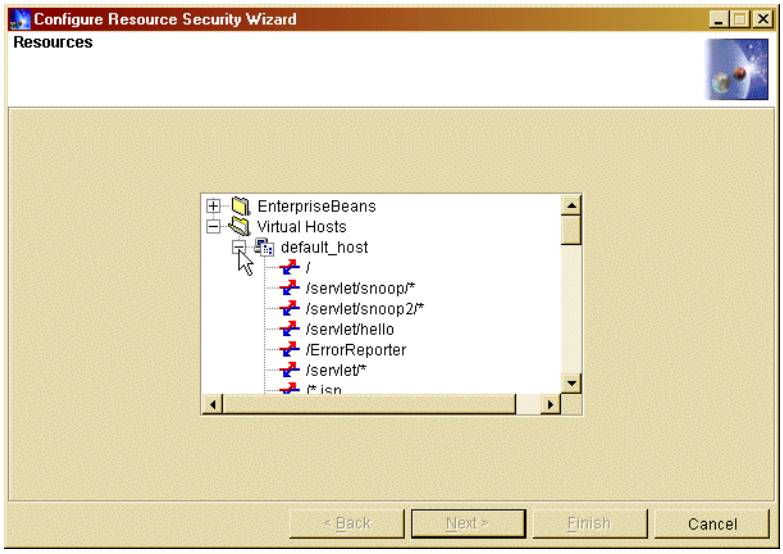

Figure 70. Configure Resource Security Wizard: Resources

__ 4. The default_host tree name is longer than what can be shown in the dialog pane. Scroll down and select **/webapp/DomApp/SimpleServlet**. Click **Next>** (Figure 71).

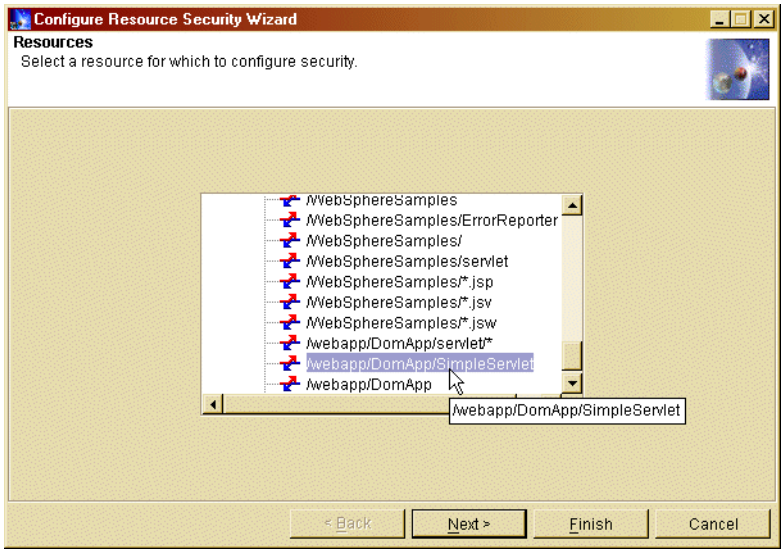

Figure 71. Configure Resource Security Wizard: Scrolling through resources

__ 5. A message appears asking to use the default method groups since no method groups have been assigned yet, click **Yes** (Figure 72).

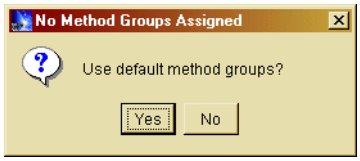

Figure 72. Configuring Resource Security to use default method groups

__ 6. On the Method Groups window, click **Finish** (Figure 73).

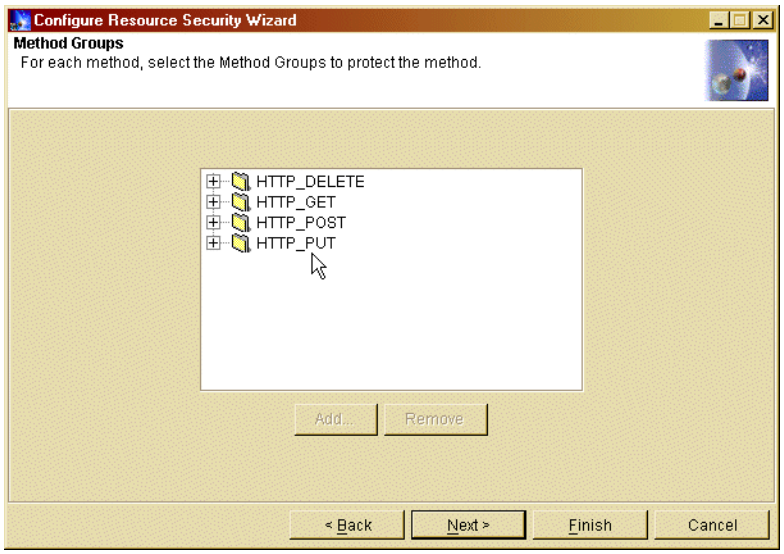

Figure 73. Configure Resource Security Wizard: Method Groups

At this point, you have protected the methods of your Web application. You still must define which users are allowed to access them. This is done by configuring Security Permissions.

Configuring Security Permissions

To assign certain users or groups access to different methods and applications, perform the following steps:

__ 1. Click the **Wizard** icon, and select **Configure Security Permissions** (Figure 74).

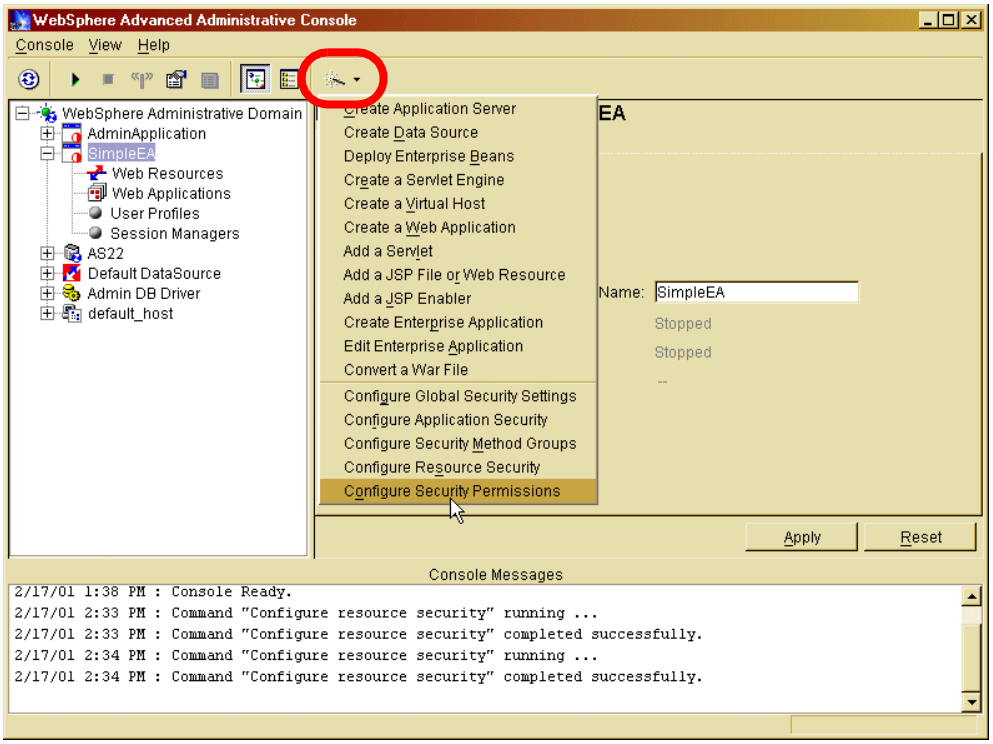

Figure 74. Configure Security Permissions

__ 2. On the Enterprise Applications window, expand the tree by clicking the plus (**+**) sign under **Enterprise Applications**.

__ 3. Select your new Enterprise Application (SimpleEA) and click **Next>** (Figure 75).

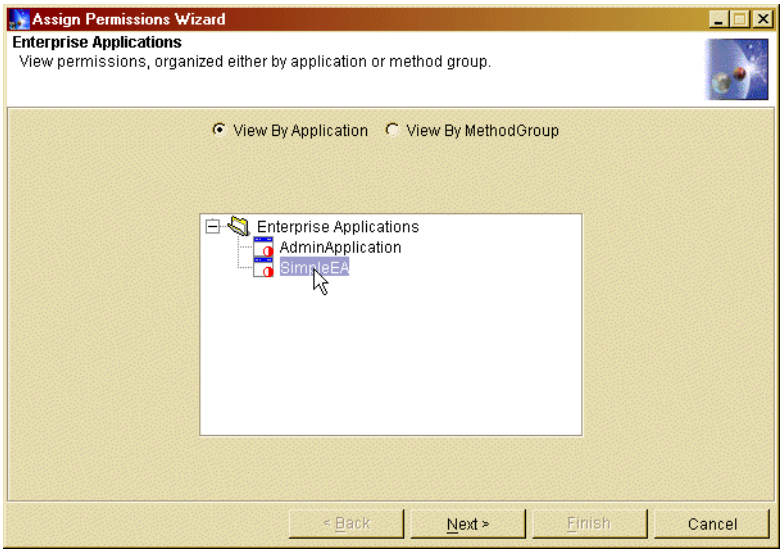

Figure 75. Assign Permissions Wizard: Enterprise Applications

__ 4. On the Permissions window (Figure 76), select all the Methods. To do so, click the first method, hold down the Shift key, and click the last method.

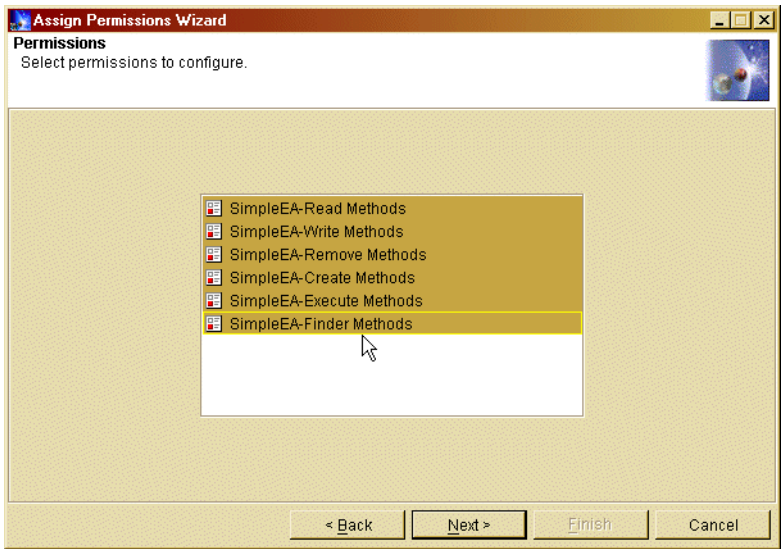

Figure 76. Assign Permissions Wizard: Selecting Permissions to configure

__ 5. Click **Next>**.

__ 6. On the Grant Permissions window, click **All Authenticated Users** (Figure 77).

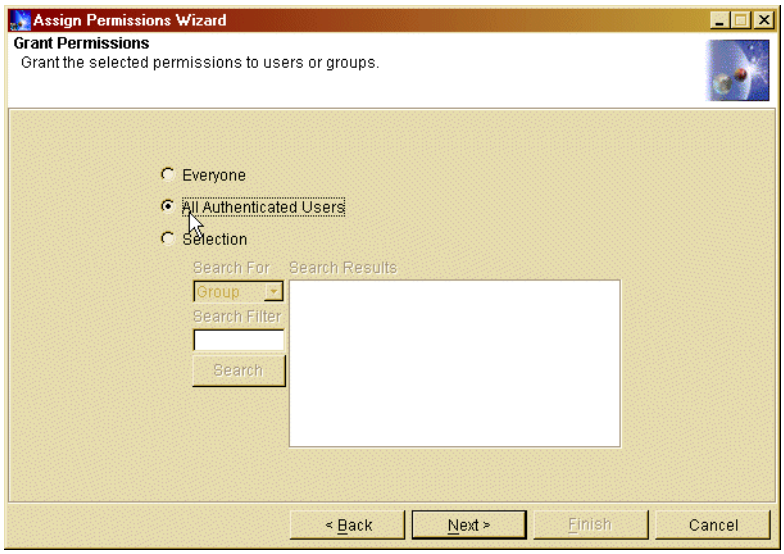

Figure 77. Assign Permissions Wizard: Grant Permissions

Note

With WebSphere Application Server 3.5.2 and Lotus Domino 5.0.6a, Single Sign-On does not allow you to protect resources for individual users. You can use either All authenticated Users (as in this example), or you can grant authority to a group.

The panel shown in Figure 77 can also be used to verify whether you have access to the correct entries in the LDAP directory. To do this, click the

Selection radio button, select **User** in the Search For pull-down menu, type * in the Search Filter field, and click **Search**.

However, for the purpose of this exercise, make sure to select **All Authenticated Users** before you click **Next>**.

__ 7. On the Remove Permissions window (Figure 78), click **Finish** to continue.

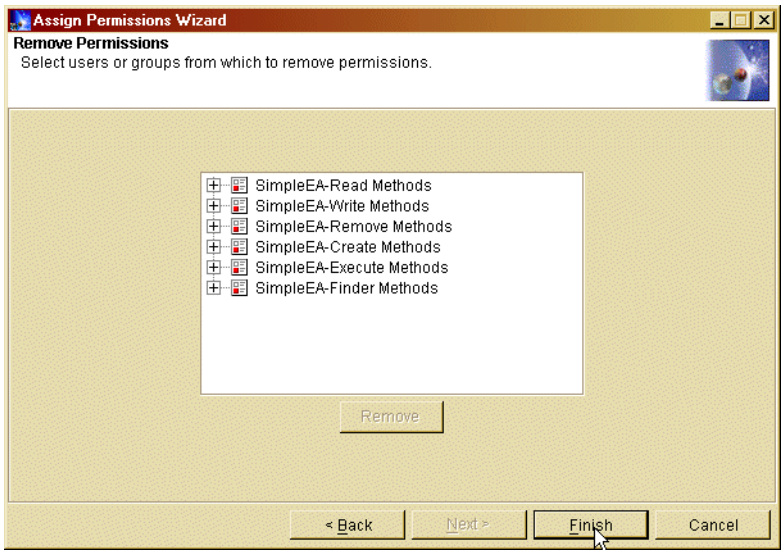

Figure 78. Assign Permissions Wizard: Remove Permissions

__ 8. The following message in the Console Messages pane appears:

```
Command "Configure permissions" completed successfully.
```

Starting SimpleEA

To activate the security settings you configured in the previous section, the SimpleEA Enterprise Application must be started.

__ 1. Right-click **SimpleEA** and select **Start** (Figure 79).

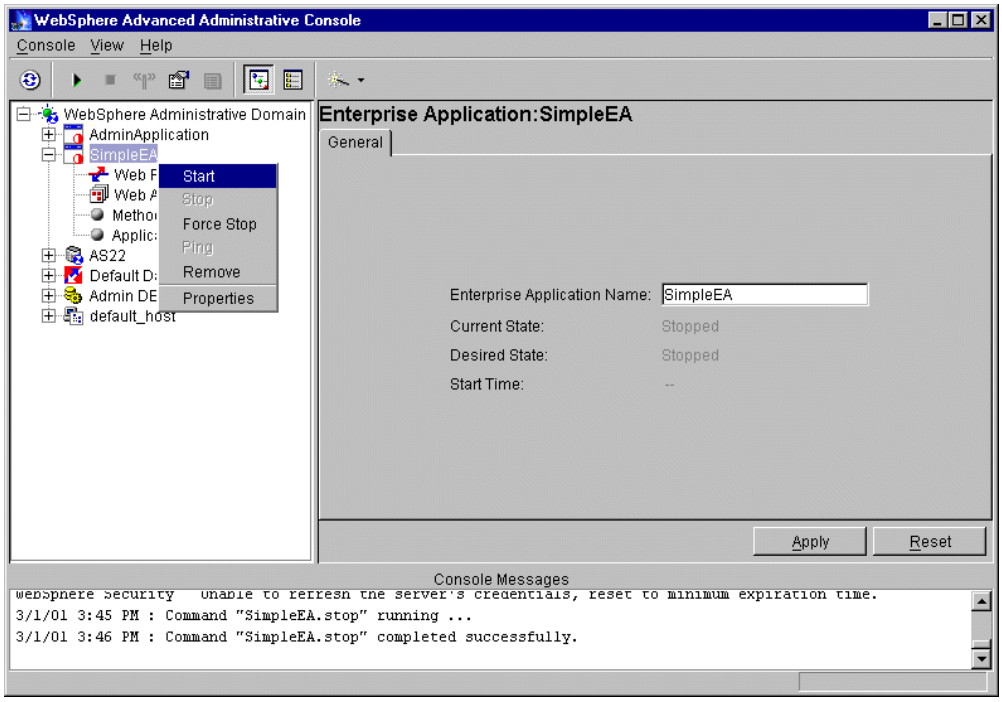

Figure 79. Start Enterprise Application: SimpleEA

__ 2. It will take at least ten minutes, until the successful completion message appears. Click **OK** (Figure 80).

Figure 80. Start SimpleEA completed successfully

Task 4: Verifying WebSphere security

Now that your servlet has been secured on the WebSphere Application Server 3.5.2, you can test it by opening the URL through a Web browser.

__ 1. Open your Netscape browser and enter the following URL:

```
http://PWDI.PID.IBM.COM:80xx/webapp/DomApp/SimpleServlet
```

__ 2. You are prompted to sign on. Enter your user name (`nguru`) and password (`dom2was`) as shown in Figure 81. Click **OK**.

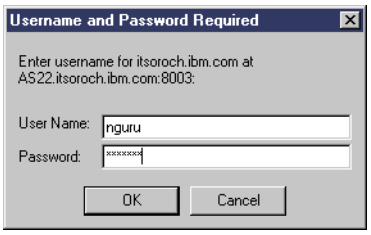

Figure 81. SimpleServlet sign on

__ 3. You are prompted to accept a cookie (Figure 82). Click **OK**.

Figure 82. Cookie

The SimpleServlet Web page appears (Figure 83).

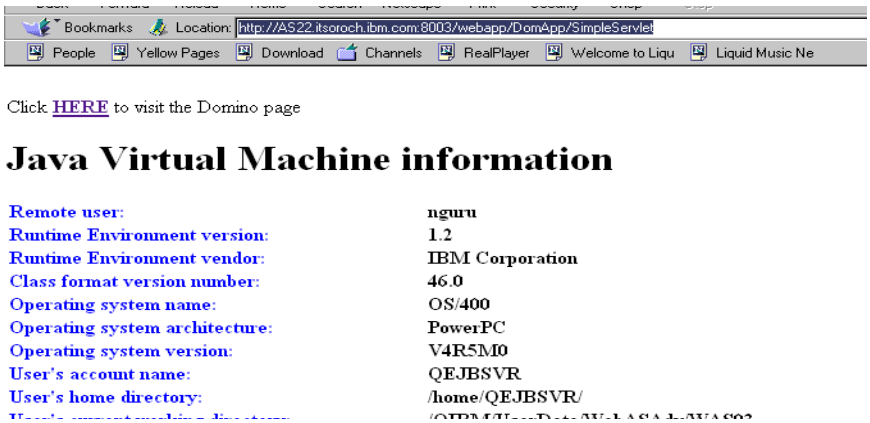

Figure 83. SimpleServlet

__ 4. To access the Domino application from the servlet, click the link:

```
Click HERE to visit the Domino page
```

Since you have not yet enabled the Single Sign-On ability between WebSphere and Domino, you are prompted by Domino to sign on again to access the Domino application (Figure 84).

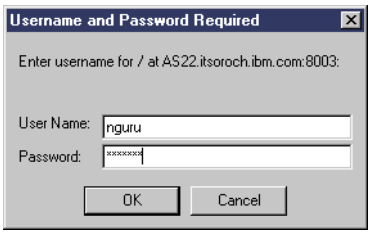

Figure 84. Sign on to the Domino application

__ 5. The Domino loan application window appears (Figure 85).

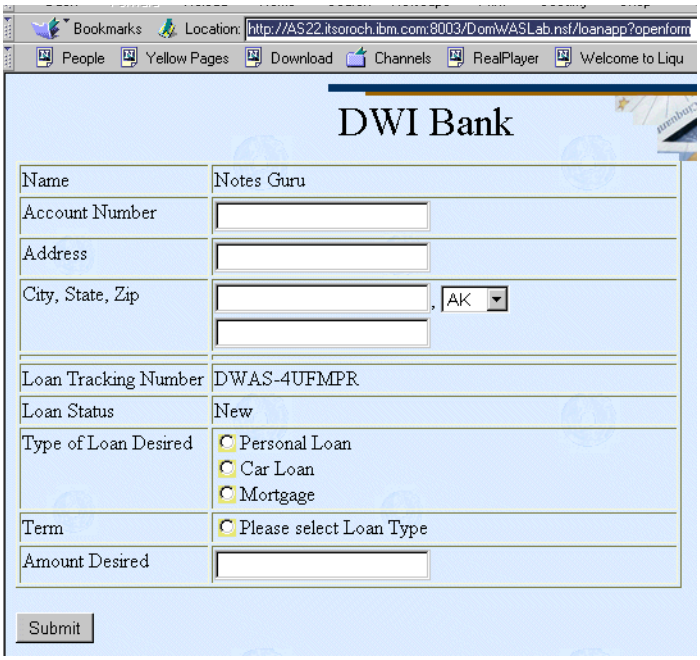

Figure 85. Domino Loan application

__ 6. Verify that you can now go back and forth between the Domino application and the WebSphere servlet without having to sign on to either environment again.

__ 7. Close the Netscape browser window.

Lab 5. Configuring Single Sign-On for WebSphere and Domino

In the previous labs, you enabled security for WebSphere Application Server 3.5.2 and Domino. To prepare to use the Single Sign-On (SSO) abilities for WebSphere and Lotus Domino for AS/400, you must update the WebSphere Global Security configuration again with Single Sign-On enabled, and re-generate and export the LPTA keys to be used when you configure Lotus Domino for AS/400 for Single Sign-On.

Configuring SSO for Domino is accomplished by selecting a new multi-server option in the Domino Server document for session-based authentication. You must also create a new domain-wide configuration document in the Domino Directory called the Web SSO Configuration document. The Web SSO Configuration document, which should be replicated to all Domino servers participating in the SSO domain, is encrypted for participating Domino servers and contains a shared secret used by Domino servers for authenticating user credentials.

Note: Before you configure Domino for Single Sign-On with WebSphere, you must configure WebSphere first because the keys generated by WebSphere have to be imported into Domino.

Objectives

This lab teaches you how to:

- Enable WebSphere Single Sign-On and export the LTPA keys.
- Create the Domino Web Single Sign-On configuration document.
- Configure the Domino Server document for Single Sign-On.
- Verify Single Sign-On works between WebSphere and Domino.

Important

Throughout these lab exercises, replace *xx* with your team number. Also refer to Table 1 on page 4 to make sure the correct values for the configuration parameters are entered.

Task 1: Configuring WebSphere for Single Sign-On

To use SSO with Domino and WebSphere application servers, you must first configure SSO for WebSphere. SSO for WebSphere allows authentication information to be shared across multiple WebSphere administrative domains and with Domino servers.

__ 1. In the WebSphere Administrative Console, click the **Wizards** icon and select **Configure Global Security Settings** (Figure 86).

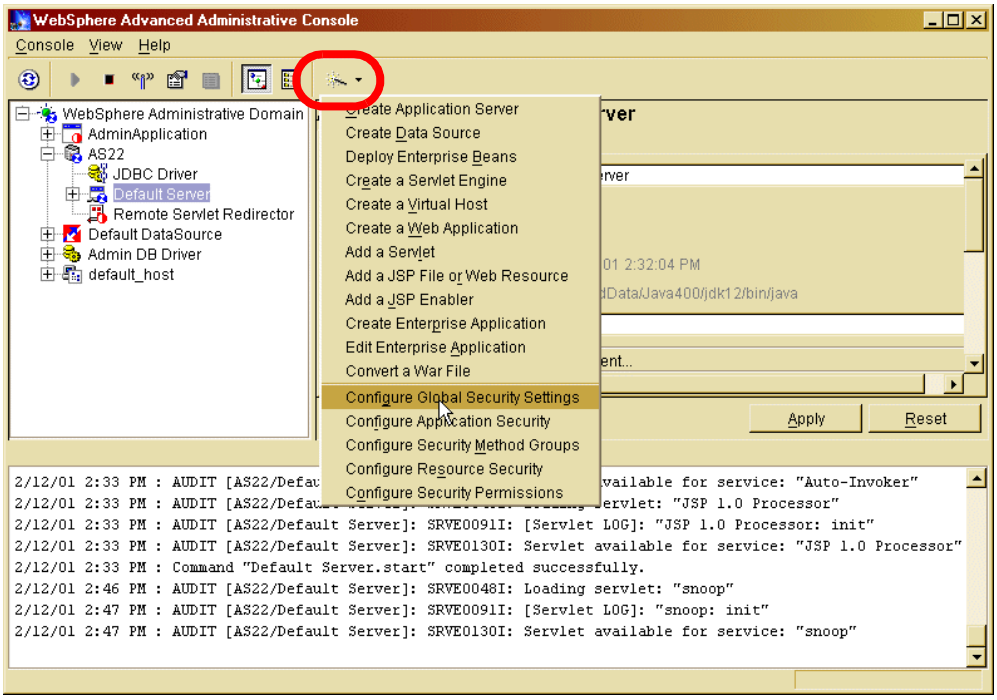

Figure 86. Configure Global Security Settings

Because you previously configured WebSphere Global Security Settings, there are only a couple of things that need to be changed.

__ 2. Click the **Authentication Mechanism** tab (Figure 87).

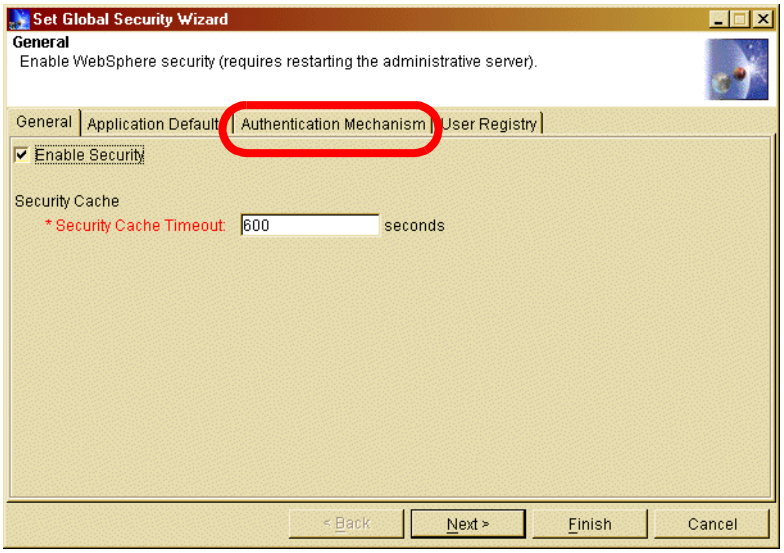

Figure 87. Global Security Settings: General tab

__ 3. On the Authentication Mechanism window (Figure 89):

a. Ensure that Lightweight Third Party Authentication (LTPA) is selected.

b. Select the **Enable Single Sign On (SSO)** box to enable SSO and authentication information to be placed in HTTP cookies.

c. Set Domain to the domain portion of your fully qualified Internet name. In your case, this is `PID.IBM.COM`.

   Note: WebSphere Application Server treats the DNS domain as case-sensitive, so ensure that the DNS domain value is specified exactly the same, including casing, whenever you use the value.

d. Re-generate the LTPA keys to be used by the WebSphere administrative domain that you are configuring. Click the **Generate Keys** button to generate keys for LTPA.

e. When prompted, enter the LTPA Password (use `dom2was`). This password is associated with the LTPA keys. Click **OK** to save the LTPA keys (Figure 88).

   Remember this password because it is used later when importing these keys while configuring SSO for Domino.

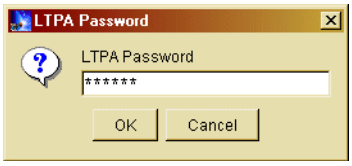

Figure 88. LTPA keys password

__ 4. Make sure, you see the message *Command "Generate LTPA Keys" completed successfully* in the Console Messages window, then click **Finish** to save the updated Global Security settings.

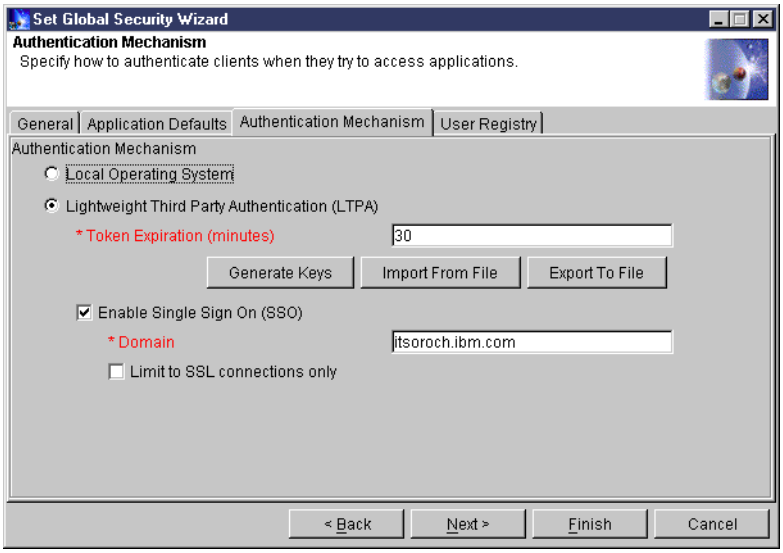

Figure 89. Global Security setting: Authentication Mechanism for SSO

__ 5. Click **OK** on the information message dialog window that warns about changes not taking effect until the administrative server is restarted (Figure 90).

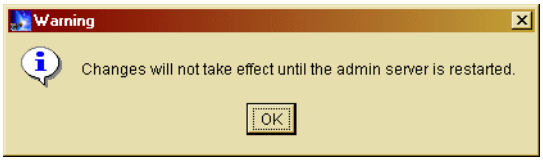

Figure 90. Changing security: Warning dialog box

__ 6. Right-click your **PWDI** node, and select **Restart** (Figure 91).

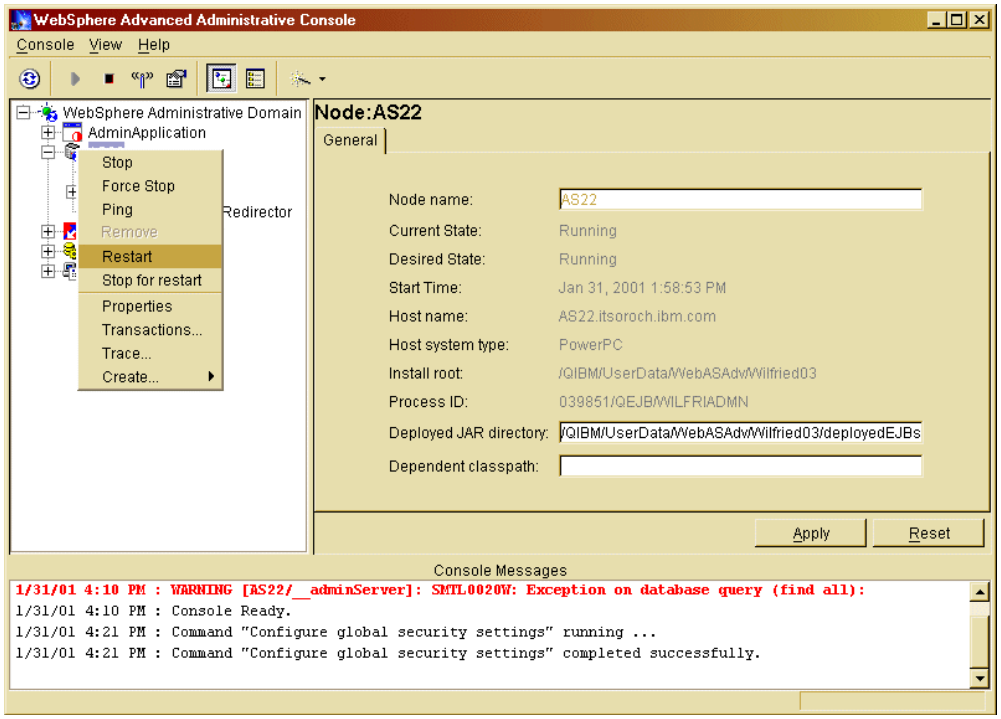

Figure 91. Restarting the administrative server

__ 7. Click **Yes** on the confirmation dialog box (Figure 92).

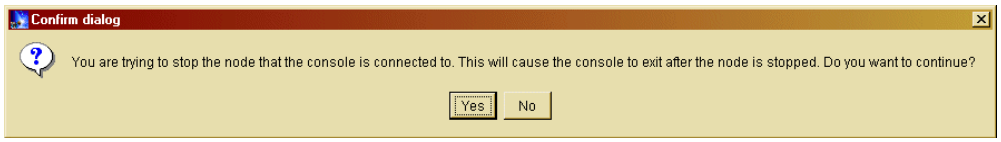

Figure 92. Restart warning dialog box

__ 8. Monitor the WASxxADMN administrative server task (or job) from the Work with Active Jobs screen (WRKACTJOB) to ensure that the WebSphere Administrative server restarts successfully. As you watch the Administrative server job, notice that it stops, starts, stops, and then starts again. This is expected after Global Security Settings have been changed. The entire process may take five minutes or more.

__ 9. Once the WebSphere Administrative Server has successfully and completely restarted, start the WebSphere Administrative Console. Specify the user ID and password exactly as you configured previously for the Security Server ID and Security Server Password fields in the Global Security Settings (Figure 93).

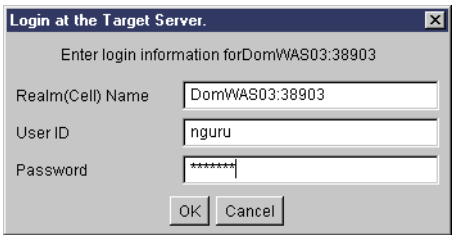

Figure 93. Sign on to the WebSphere Administrative Console

To complete the WebSphere security configuration for SSO, export the LTPA keys to a file. This file is used later when importing keys into the Domino Web SSO configuration document.

__ 1. On the WebSphere Administrative Console, click the **Wizards** icon and select **Configure Global Security Settings**.

__ 2. Click the **Authentication Mechanism** tab.

__ 3. Click the **Export To File** button to export the LTPA keys to a file.

__ 4. On the Export to File window, specify a `LTPA Keys` filename and `C:\Temp` for location to contain the LTPA keys. Any file name and extension works. However, be sure you remember it since you use it later (Figure 94).

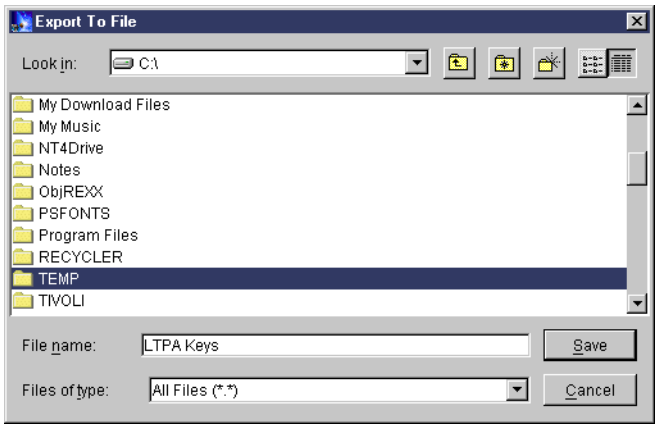

Figure 94. Exporting LTPA keys to a file

__ 5. Click **Save** to save the file.

__ 6. Click **Cancel** to close the Global Security Settings wizard.

Task 2: Creating the Domino Web Single Sign-On configuration document

To create the Domino Web SSO Configuration document, use a Notes Client R5.0.5 (or later) and perform the following tasks.

Note

When you perform the following steps with a Notes client, which has already been used in a different environment (that is, with a different Domino server), you need to make sure, the location document of your Notes client points to the Domino server where you want to enable SSO. This is needed so that public key can be used for the server. If a message appears when you save the Web SSO Config document saying it could not find server, then this should fix the message. Otherwise, if you try starting the HTTP server after enabling Mult-Server in Session authentication then you will get the Error Loading Web SSO configuration message when HTTP is stared.

You may also have to add server names.nsf to existing NAMES= line in Notes.ini of your Notes client as follows:

NAMES=names.nsf,CN=DOMWASxx/O=Domxx!!names.nsf

__ 1. From the Lotus Notes client, open the **Domino Directory** database names.nsf on your server DOMWASxx and select the **Servers** view.

__ 2. Click the **Web...** pull-down menu and select the **Create Web SSO Configuration** button to create the document (Figure 95).

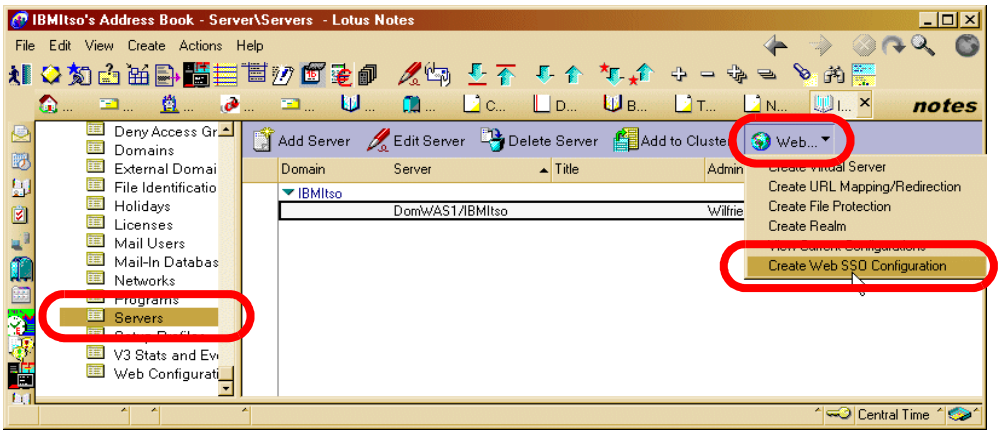

Figure 95. Selecting Create Web SSO Configuration from the Web... pull-down menu

__ 3. In the Web SSO Configuration document, click the **Keys...** pull-down menu as shown in Figure 96.

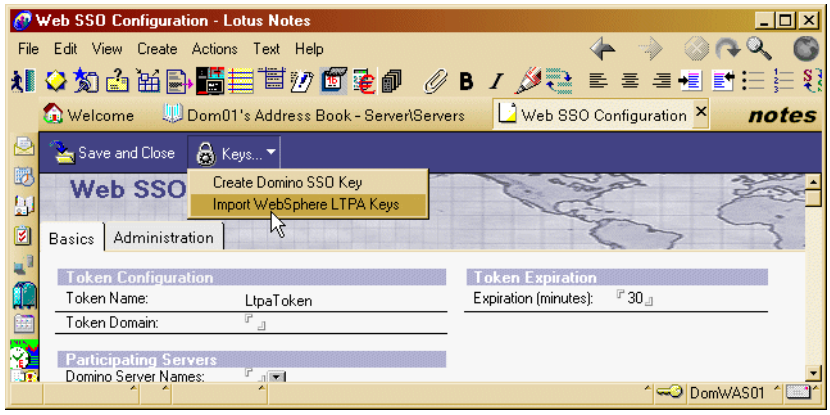

Figure 96. Selecting Keys->Import LPTA Keys from the Web SSO Document

__ 4. Select **Import WebSphere LTPA Keys** to import the LTPA keys from a file.

__ 5. Enter the path to the LTPA Keys file that was exported earlier. Enter `c:\temp\LTPA Keys` and click **OK** (Figure 97).

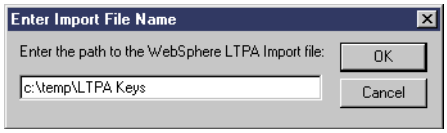

Figure 97. Entering the import file name for LTPA keys

__ 6. Enter the password that you used earlier (`dom2was`) when generating the LTPA Keys (Figure 98).

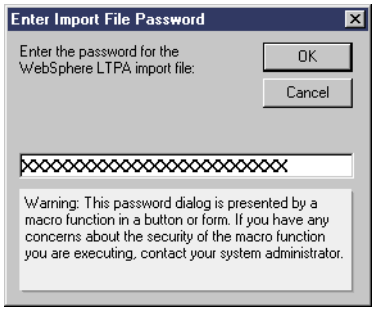

Figure 98. Enter LTPA keys password

__ 7. Click **OK** on the successful import message window (Figure 99).

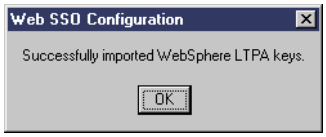

Figure 99. Imported LTPA keys successful

__ 8. The Web SSO Configuration document should automatically be updated to reflect the information from the LTPA Keys file you just imported.

__ 9. Figure 100 shows the Web SSO Configuration document. Update the fields in this document as follows:

- **Token Domain = PID.IBM.COM**

  This is the DNS domain portion of the fully qualified Internet name of your system. Because all servers participating in SSO must be in the same DNS domain, this value must be the same as the Domain value specified when configuring WebSphere Application Server.

  Note: WebSphere Application Server treats the DNS domain as case-sensitive, so ensure that the DNS domain value is specified exactly the same, including casing, whenever you use the value.

- **Domino Server Names = DOMWASxx/Domxx** (*xx* = team number)

  These are the Domino servers that participate in SSO. You must specify a fully qualified Domino server name here (for example, MyDominoServer/MyOu).

- **LDAP Realm = DOMWASxx.PID.IBM.COM\:389xx** (*xx* = team number)

  This is the fully qualified host name of the LDAP server. This field is initialized from the information provided in the LTPA keys file.

  Note: You only need to change this value if an LDAP server port value is specified for the WebSphere administrative domain (which is the case for this lab). If a port is specified, a backslash (\) must be inserted in the value before the colon. For example, replace `mymachine.mydomain.ibm.com:389` with `mymachine.mydomain.ibm.com\:389`.

- **Token Expiration = <leave default>**

  This is the number of minutes a token can exist before expiring. A token does not expire based on inactivity. Rather, it is valid for only the number of minutes specified from the time of issue.

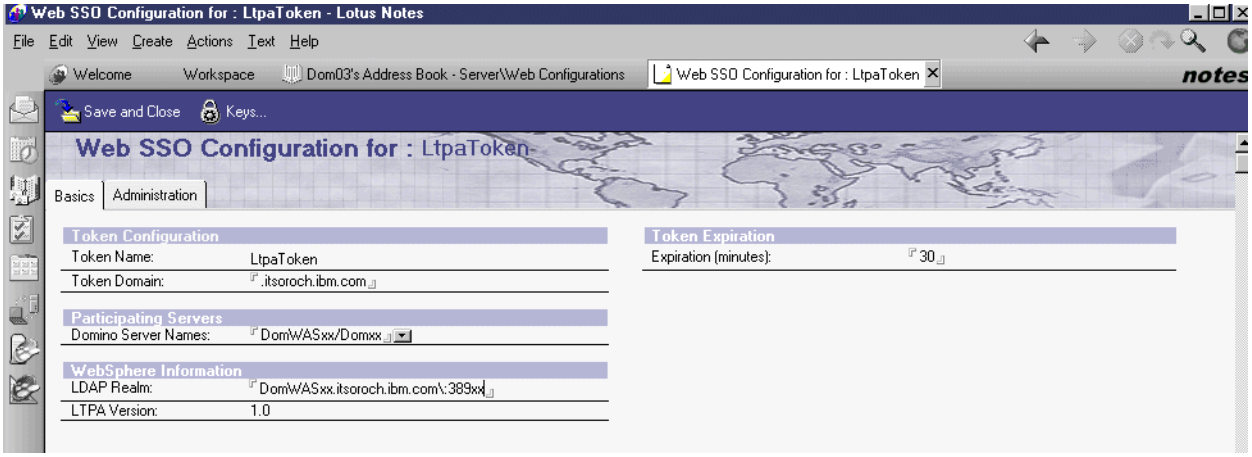

Figure 100. Domino Web SSO Configuration document

Save and close the Web SSO Configuration document. It now appears in the Web Configurations view.

Task 3: Configuring the Domino Server document for Single Sign-On

To update the Domino Server document for SSO, perform the following tasks:

__ 1. In the Domino Directory, edit the server document. See Figure 101.

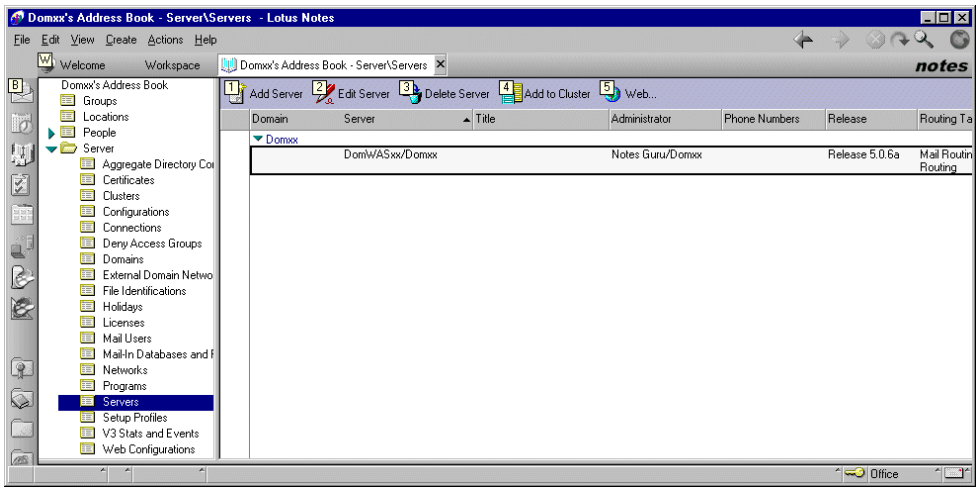

Figure 101. Domino server view

__ 2. Select the **Ports** tab, select the **Internet Ports** tab, and then select the **Web** tab. See Figure 102.

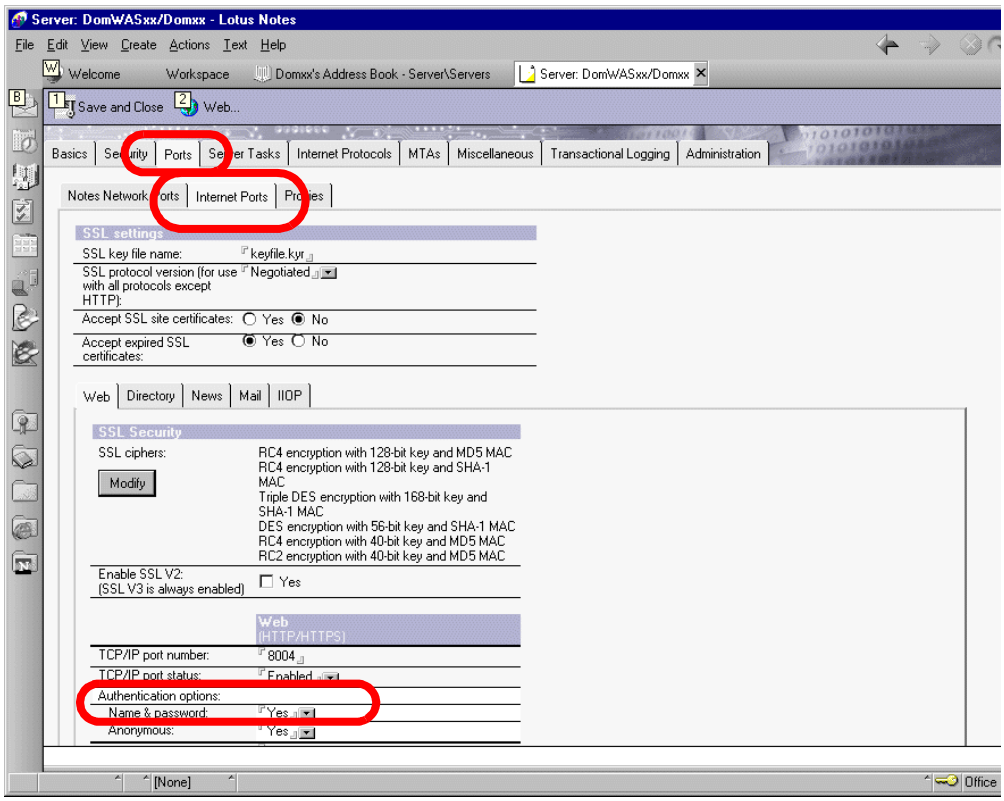

Figure 102. Ports, Internet Ports, and Web tabs selected

__ 3. Ensure that the Name & Password field in the TCP/IP Authentication options is set to **Yes**. This enables basic authentication for Web users. See Figure 102.

__ 4. Select the **Internet Protocols** tab, and then select the **Domino Web Engine** sub-tab (Figure 103).

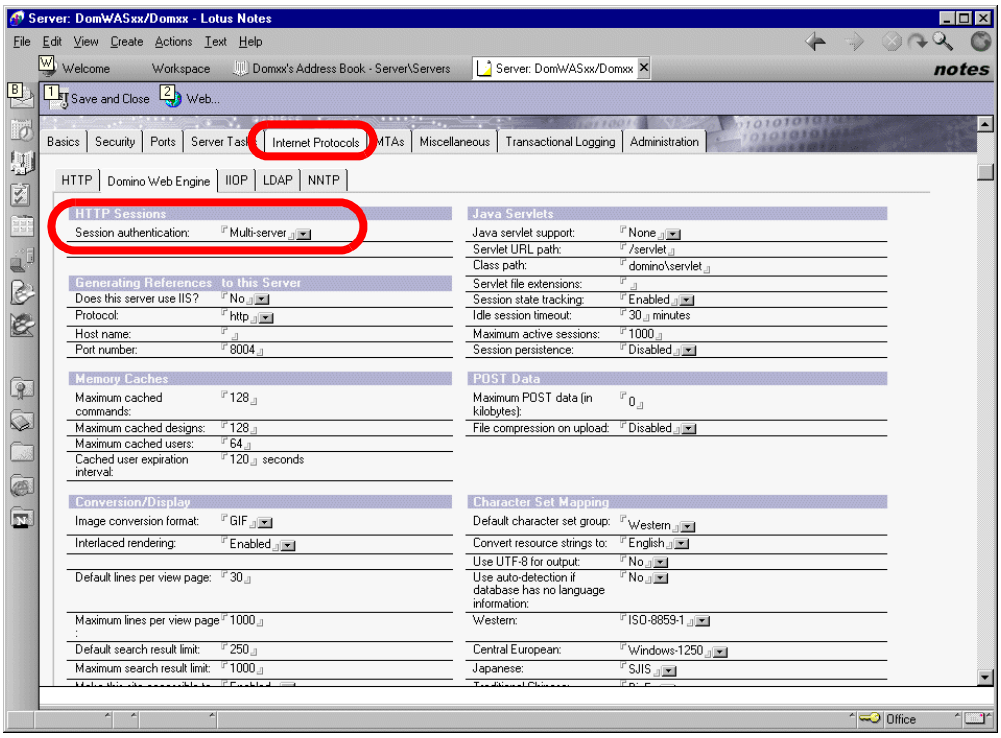

Figure 103. Selecting Internet Protocols and the Domino Web Engine

__ 5. In the HTTP Sessions section, click the drop-down menu in the Session authentication field and select **Multi-server**. This enables SSO for Domino (Figure 103).

__ 6. Press **Save and Close** to close the Server document.

__ 7. For these changes to take effect, the Domino server must be stopped and restarted. To do this, from your 5250 session, enter the `following` command and press Enter:

```
WRKDOMSVR DOMWASxx
```

__ 8. From the Work with Domino Servers screen, enter option `6` (End Server) next to your Domino server.

__ 9. Refresh the screen to verify that the Domino server is ended by pressing F5 until the status is *ENDED.

__ 10. Enter option `1` (Start Server) next to your Domino server to start it again.

__ 11. You must now start your Domino HTTP server. Wait until the server shows status *Started*. Then, from the Work with Domino Servers screen, enter option `8` (Work Console) to go into the Domino server console.

__ 12. Enter the `load http` command to start the Domino HTTP server task. Press F5 to refresh the screen and verify that the HTTP task starts successfully. You should see the following message:

```
Successfully loaded Web SSO configuration
```

__ 13. You must now start your Domino LDAP server. From the Domino console display, enter the following command to start the Domino LDAP server task:

```
load ldap
```

__ 14. Press F5 to refresh the screen and verify that the LDAP task starts successfully.

__ 15. Press F3 to exit the Domino console.

Task 4: Verifying Single Sign-On between WebSphere and Domino

At this point, you are ready to verify that SSO for WebSphere and Domino is configured and working correctly.

You must first test opening the servlet in WebSphere and then link to the Domino application. You should only be prompted to sign on once when initially going to the SimpleServlet. After that, you are able to move back and forth between the two applications without being prompted to sign on.

The second test is to go the Domino application and then link to the SimpleServlet in WebSphere. Again, you should only be prompted once when initially going into the Domino application. After that, you should again be able to move back and forth between the two applications without being prompted to sign on.

SimpleServlet to Domino application SSO test

Perform the following tasks to test the SimpleServlet to Domino application SSO:

__ 1. Open your Netscape browser and enter the following URL:

```
http://PWDI.PID.IBM.COM:80xx/webapp/DomApp/SimpleServlet
```

__ 2. You are now prompted to sign on. Enter your user name (`nguru`) and password (`dom2was`) as shown in Figure 104. Click **OK**.

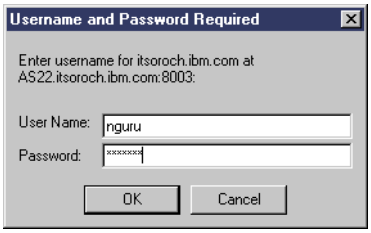

Figure 104. SimpleServlet sign on

__ 3. You are prompted to accept a cookie. This cookie is generated as a result of SSO. Click **OK**. Note, if you do not see the SSO Cookie as shown in

Figure 105, but only the one as shown in Figure 106, your Single Sign-On configuration is not correctly working!

Figure 105. SSO Cookie

__ 4. You are now prompted to accept another cookie (Figure 106). This is the original cookie that you saw before enabling SSO. Click **OK**.

Figure 106. Cookie

__ 5. The SimpleServlet Web page appears (Figure 107).

Click HERE to visit the Domino page

Java Virtual Machine information

Remote user:	nguru
Runtime Environment version:	1.2
Runtime Environment vendor:	IBM Corporation
Class format version number:	46.0
Operating system name:	OS/400
Operating system architecture:	PowerPC
Operating system version:	V4R5M0
User's account name:	QEJBSVR
User's home directory:	/home/QEJBSVR/
User's current working directory:	/QIBM/UserData/WebASAdv/WAS03
Class path:	/QIBM/ProdData/java400/ext/db2_classes.jar

Figure 107. SimpleServlet Web page

__ 6. To access the Domino application from the servlet, click on the link:

```
Click HERE to visit the Domino page
```

Because you have enabled the Single Sign-On capability between WebSphere and Domino, you should not be prompted by Domino to sign

on again to access the Domino application. Rather, you should be taken directly into the Domino application (Figure 108).

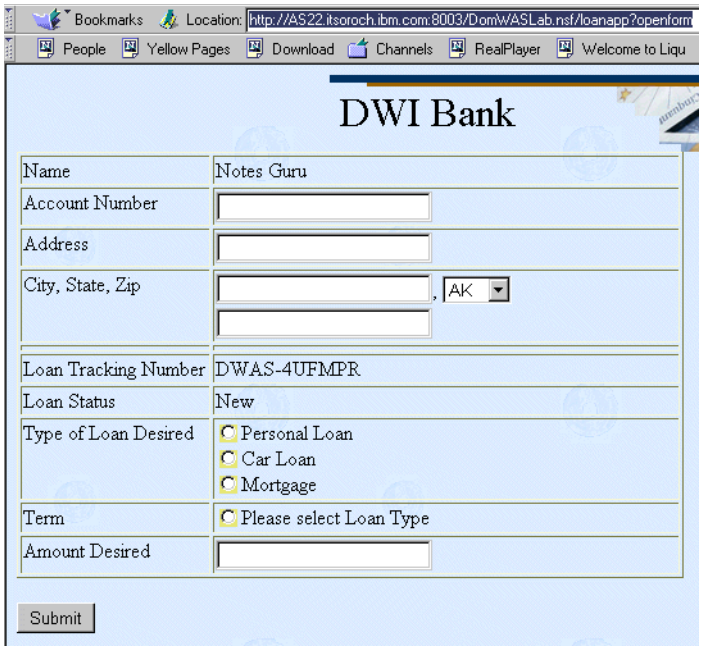

Figure 108. Domino application

Domino application to SimpleServlet SSO test

Perform the following tasks to test the Domino application to SimpleServlet SSO:

__ 1. Close your Netscape browser window and re-open it to remove the cookies that were set in the previous test.

__ 2. From the Netscape browser, go to the Domino Web application (DomWASLab.nsf) by entering the following URL (remember to replace *xx* with your team number):

```
http://PWDI.PID.IBM.COM:80xx/DomWASLab.nsf/loanapp?openform
```

__ 3. The Web page shown in Figure 109 on page 86 should appear asking for a valid user name and password. Enter the user name (`nguru`) and password (`dom2was`) and click **Login**.

Figure 109. Domino SSO challenge

__ 4. You are prompted to accept a cookie (Figure 110). This cookie is generated as a result of SSO. Click **OK**.

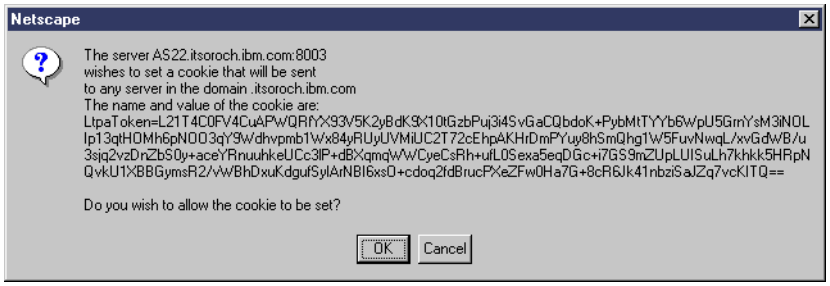

Figure 110. SSO Cookie

__ 5. The Domino application appears (Figure 111).

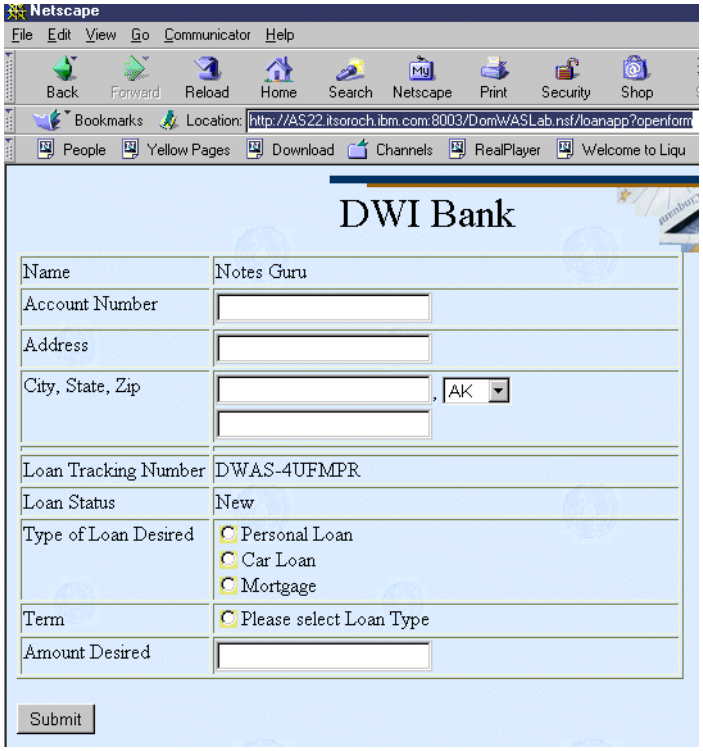

Figure 111. Domino loan application

__ 6. Click the **Submit** button to get to the link to the WebSphere SimpleServlet.

__ 7. On the next Web page that appears (Figure 112), click on the link:

`Return to the Main Menu`

This will take you to the WebSphere SimpleServlet.

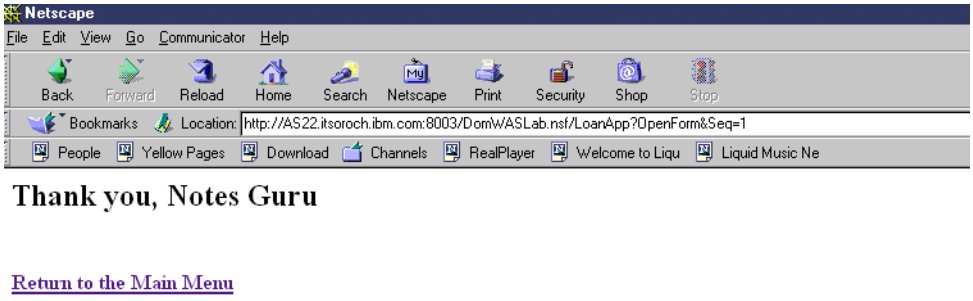

Figure 112. Domino application link to SimpleServlet

__ 8. Again, because you have enabled the Single Sign-On ability between WebSphere and Domino, you should not be prompted by WebSphere to sign on again to access the SimpleServlet. Howver, you are now prompted to accept another cookie (Figure 113). This is the original cookie that you saw before enabling SSO. Click **OK**.

Figure 113. Cookie

__ 9. The WebSphere SimpleServlet should appear (Figure 107 on page 84).

__ 10. When you are finished testing, close the Netscape browser window.

Congratulations! You have successfully completed the lab.

This concludes the main portion of the Domino and WebSphere Integration on iSeries server lab. If you have time, or are interested, there are two additional optional labs:

- Lab 6. “Optional lab: Using the OS/400 LDAP server” on page 91, takes you through the steps required for changing your environment to use the OS/400 LDAP server instead of the Domino LDAP.
- Lab 7. “Optional lab: Using IBM HTTP Server for OS/400” on page 113, takes you through the necessary steps for switching from using the Domino HTTP server to using the OS/400 HTTP server.
- Lab 8. “Information only: Configuring the OS/400 LDAP server” on page 129, is for informational purposes only. It contains the steps required to configure OS/400 LDAP and how to publish entries in the System Distribution Directory to the OS/400 LDAP directory.

Part 3. Appendices

Part 3 contains optional labs that you can do if there is time remaining.

Lab 6. “Optional lab: Using the OS/400 LDAP server” on page 91, explains how to use OS/400 LDAP instead of the Domino LDAP that was used in the main portion of the lab.

Lab 7. “Optional lab: Using IBM HTTP Server for OS/400” on page 113, explains how to switch from using the Domino HTTP server that was used in the main portion of the lab to using the OS/400 HTTP server.

Lab 8. “Information only: Configuring the OS/400 LDAP server” on page 129, is for informational purposes only. It provides information on how to configure OS/400 LDAP, and how to publish entries in the System Distribution Directory to the OS/400 LDAP directory.

Lab 6. Optional lab: Using the OS/400 LDAP server

During the previous lab exercises, you used Lotus Domino for AS/400 as your LDAP server. In this lab, you set up your WebSphere Application Server 3.5.2 instance and Domino server to use the OS/400 LDAP server. You then test your server setup.

Note: For the purposes of this lab, the OS/400 LDAP server has already been set up and configured. This is because only one person can perform these functions on the system. For information on how to do this, refer to Lab 8. “Information only: Configuring the OS/400 LDAP server” on page 129, which shows you how to set up and configure OS/400 LDAP.

Objectives

This lab teaches you how to:

- Check your connection to the OS/400 LDAP server.
- Change WebSphere to use OS/400 LDAP for security.
- Create a Domino Directory Assistance database to connect to OS/400 LDAP.
- Change Domino to use OS/400 LDAP for security.
- Retest your Domino and WebSphere Single Sign-On environment using OS/400 LDAP.

Important

Throughout these lab exercises, replace *xx* with your team number. Also, refer to Table 1 on page 4 to make sure the correct values for the configuration parameters are entered.

Task 1: Checking your connection to OS/400 LDAP

In this section, you check the connection to the OS/400 LDAP directory and verify that the directory entries were published from the OS/400 System Distribution Directory. There are a number of different methods for doing this. You use the Web browser and, optionally, you can use the Qshell utility.

Accessing OS/400 LDAP from a Web browser

In this section, you access OS/400 LDAP using a Web browser by performing the following tasks:

__ 1. Check whether you can establish a connection to the LDAP server. Open your Netscape browser and enter the following location:

```
ldap://PWDI/
```

__ 2. Ensure that your OS/400 user ID was published from the System Distribution Directory (SDD). Type the following information in the Netscape browser location field (replace xx by your team number):

```
ldap://PWDI/cn=Joe Bloggsxx,ou=ITSO,o=IBM,c=US
```

Accessing OS/400 LDAP from Qshell

Perform the following tasks to access OS/400 LDAP from Qshell:

__ 1. You can also use the Qshell utility to access OS/400 LDAP. To access the Qshell Interpreter, enter the Start QSH (STRQSH or QSH) OS/400 command and press Enter.

__ 2. Ensure that the LDAP Administrator password is correct by entering:

```
ldapsearch -v -D cn=Administrator -w ldappw -b cn=monitor -s base
"(objectclass=*)"
```

__ 3. Search and display all LDAP directory entries by entering:

```
ldapsearch -v -D cn=Administrator -w ldappw -b ou=ITSO,o=IBM,c=US
"(objectclass=*)"
```

Task 2: Changing WebSphere to use OS/400 LDAP

To use OS/400 LDAP for SSO with Domino and WebSphere application servers, you must first change the WebSphere configuration.

__ 1. From the WebSphere Administrative Console, click the **Wizards** icon, and select **Configure Global Security Settings** (Figure 114).

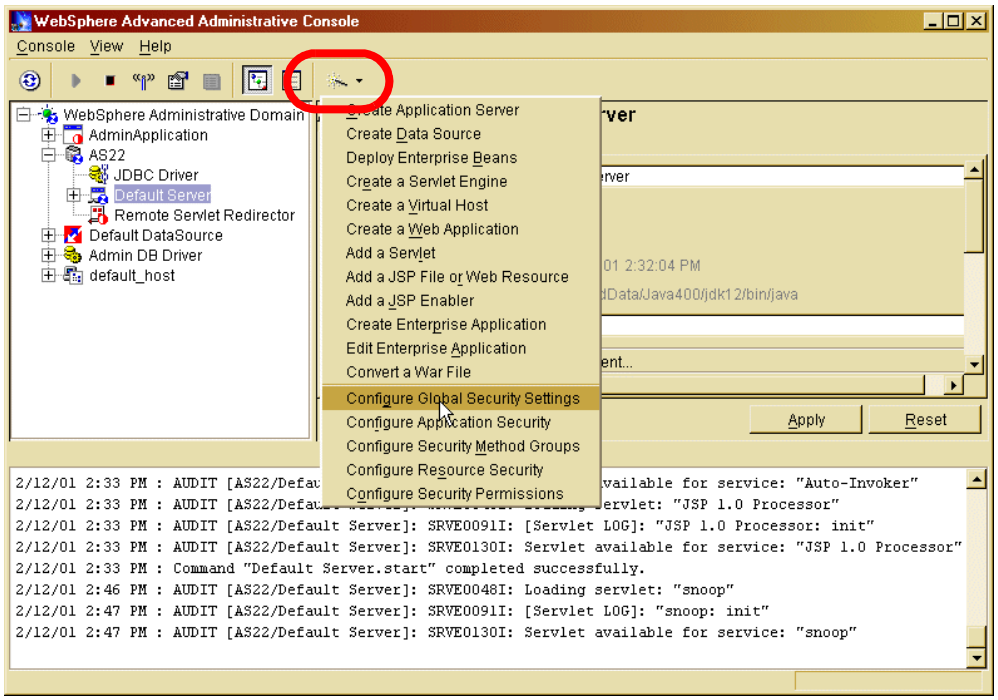

Figure 114. Configure Global Security Settings

Because you previously configured the WebSphere Global Security Settings, there are only a couple of things that need to be changed.

__ 2. From the Global Security Setting window, click the **User Registry** tab. The user registry must be an LDAP directory managed by an LDAP server that is currently running (the wizard attempts to connect to the LDAP server to verify the information you enter). Fill in the LDAP fields as explained in the following list (Figure 115 on page 94):

- **Security Server ID** = **DOMWASxx**

  This is the user ID of the administrator for the WebSphere administrative domain. This user ID is used later when accessing WebSphere administration services using the WebSphere Administrative Console. By default, this should be the value of the short name or user ID for a user already defined in the LDAP directory. Do *not* specify a Distinguished Name by using *cn=* or *uid=* before the value.

  Note: When you start the WebSphere Administrative Console later on, you must enter the value exactly as you specified it in this field.

- **Security Server Password** = **dom2was**

  This is the valid password for the Security Server ID. This field is case-sensitive.

- **Directory Type = SecureWay**

  This should be set for the type of LDAP server you are using. For example, select SecureWay for IBM SecureWay LDAP Directory, or Domino 5.0 for Domino LDAP directory.

- **Host = PWDI.PID.IBM.COM**

  This is the fully qualified host name on which the LDAP directory is running.

- **Port = Leave port blank**

  This is the port on which the LDAP directory runs. You may leave this field blank for the default, non-SSL (secure sockets layer) port of the LDAP directory (port 389).

- **Base Distinguished Name = ou=ITSO,o=IBM,c=US**

  This is the Distinguished Name (DN) of the directory in which searches begin within the LDAP directory. For example, for a user with a DN of cn=John Doe, ou=ITSO, o=IBM, and c=US, you could specify a base DN of ou=ITSO, o=IBM, c=US (as we do in this lab) or o=IBM, c=US or c=US. This is a required field for all LDAP directories except for the Domino Directory.

  Note: If you are using the Domino Directory, and you specify a Base Distinguished Name, you are not able to grant permissions to individual Web users for resources managed by your WebSphere application server.

- **Bind Distinguished Name = <leave this field blank>**

  This is the DN of the user who is capable of performing searches on the directory. In most cases, this field is not required since all users are usually authorized to search an LDAP directory. However, if the LDAP directory contents are protected from all LDAP users, you need to specify the DN of an authorized user, such as the administrator of the directory (for example, cn=Administrator).

- **Bind Password = <leave this field blank>**

  This is the valid password for the user specified as the Bind Distinguished Name. This is required only if you specify a value for Bind Distinguished Name. This field is case-sensitive.

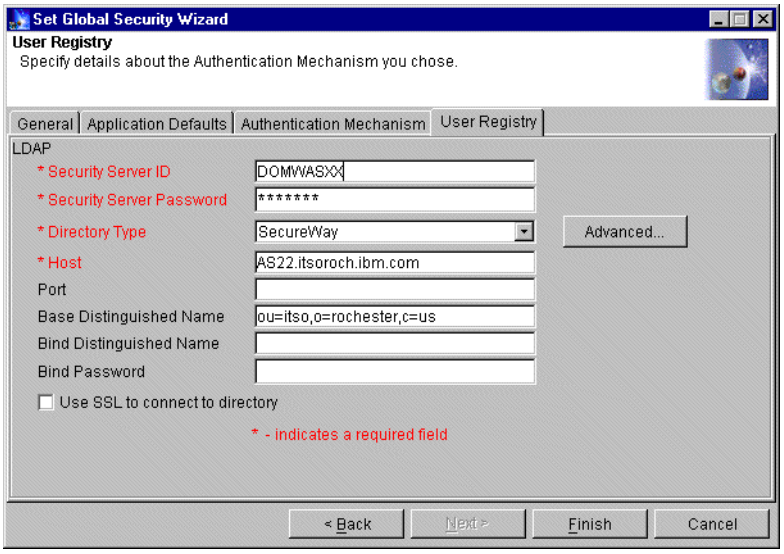

Figure 115. Set Global Security Wizard: User Registry tab

__ 3. Click **Finish** to save the Global Security Settings.

__ 4. Click **OK** on the information message dialog window warning that changes will not take effect until the administrative server is restarted (Figure 116).

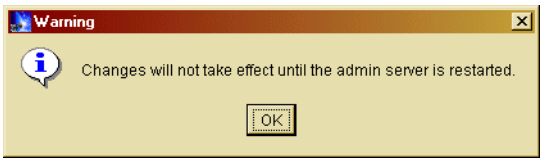

Figure 116. Changing security warning dialog box

__ 5. Right-click your **PWDI** node and select **Restart** (Figure 117).

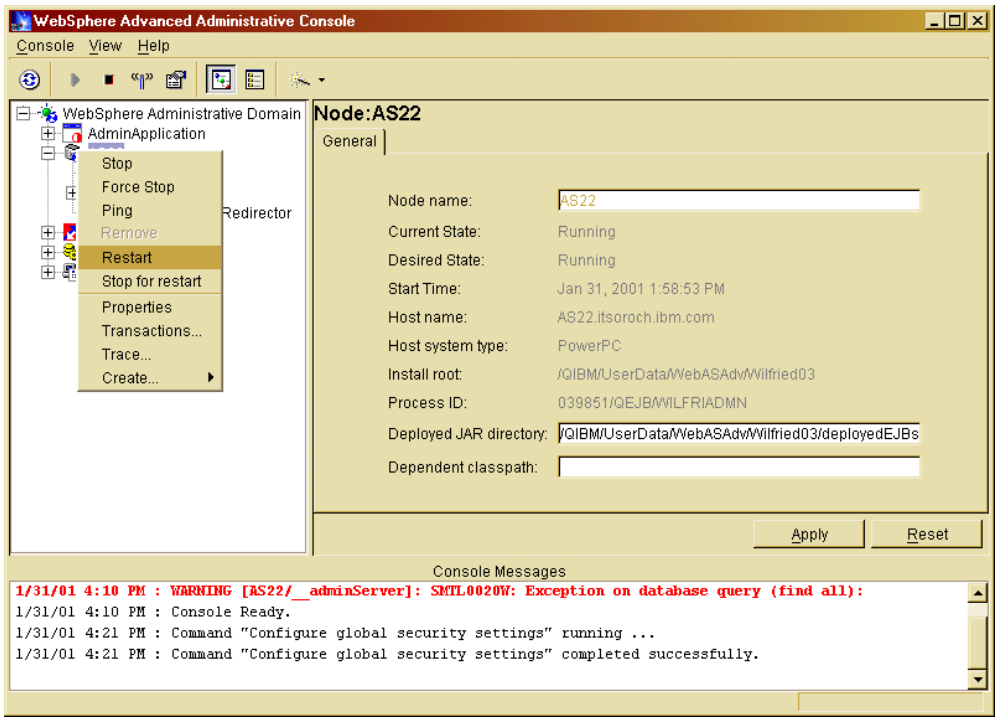

Figure 117. Restarting the Administrator server

__ 6. Click **Yes** on the confirm dialog box (Figure 118).

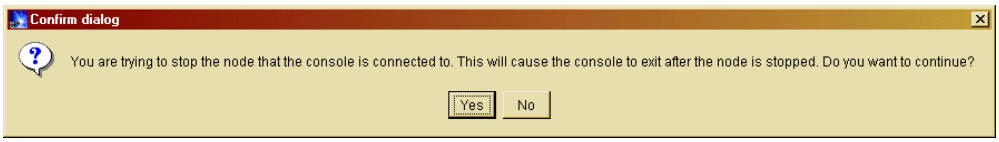

Figure 118. Restart warning dialog box

__ 7. Monitor the WASxxADMN administrative server task (or job) from the Work with Active Jobs screen (WRKACTJOB) to ensure the WebSphere Administrative server restarts successfully. While monitoring the Administrative server job, notice that it stops, starts, stops, and then starts again. This is expected after Global Security Settings have been changed.

__ 8. Once the WebSphere Administrative Server successfully and completely restarts, start the WebSphere administrative console. Specify the user ID and password exactly as you configured them previously for the Security Server ID and Security Server Password fields in the Global Security Settings wizard (Figure 119).

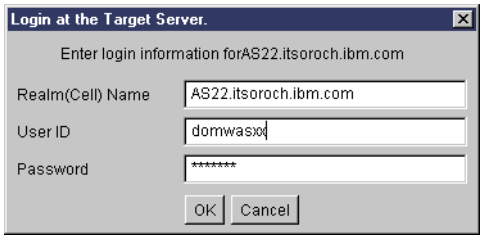

Figure 119. Sign on to the WebSphere Administrative console

__ 9. From the WebSphere Administrative Console, click the **Wizards** icon, and select **Configure Global Security Settings** (Figure 120).

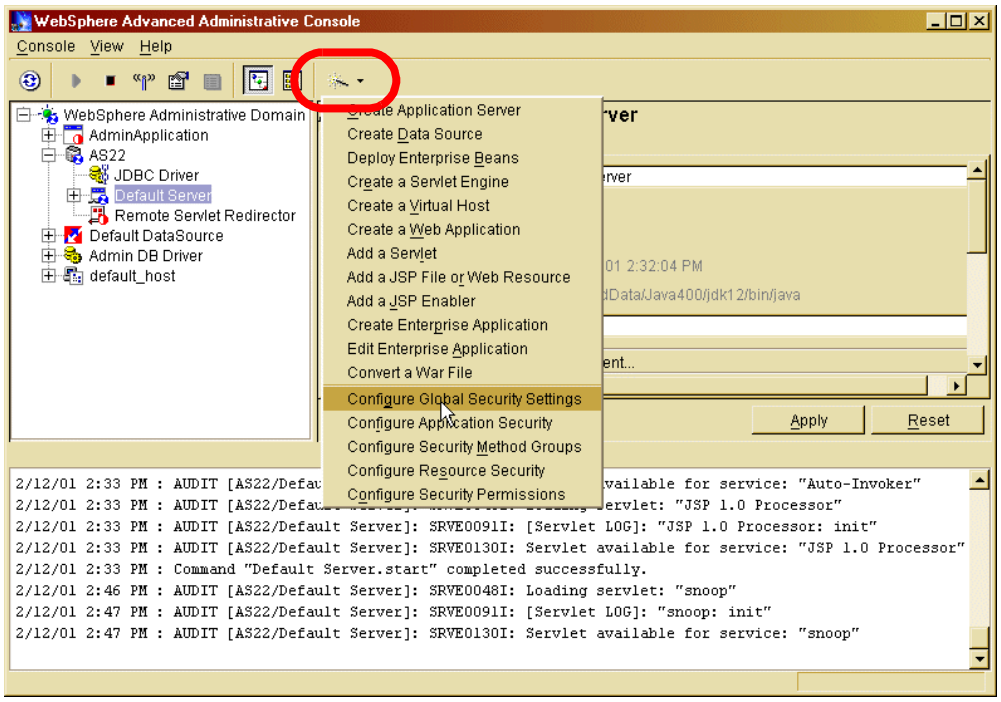

Figure 120. Configure Global Security Settings

Because you previously configured WebSphere Global Security Settings, you now only want to re-generate the LTPA keys and export them to a file so you can import them into Domino later in this lab.

__ 10. From the Global Security Settings window, click the **Authentication Mechanism** tab.

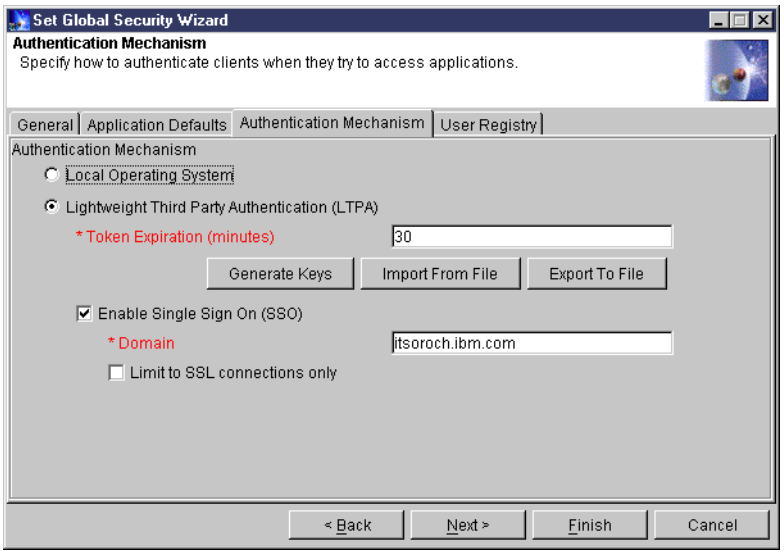

Figure 121. Set Global Security Settings Wizard: Authentication Mechanism

__ 11. On the Authentication Mechanism window (Figure 121):

a. Re-generate the LTPA keys to be used by the WebSphere administrative domain that you are configuring. Click the **Generate Keys** button to generate keys for LTPA.

b. When prompted, enter the LTPA password (`dom2was`). This password is associated with the LTPA keys. Click **OK** to save the LTPA keys (Figure 122).

Remember this password because it is used later when importing these keys while configuring SSO for Domino.

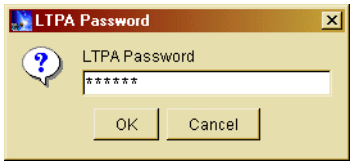

Figure 122. LTPA keys password

__ 12. Click the **Export To File** button to export the LTPA keys to a file.

__ 13. On the Export to File window, specify a filename (`LTPA Keys`) and a location (`C:\Temp`) to contain the LTPA keys. Any file name and extension works. However, remember the extension because you use it later (Figure 123).

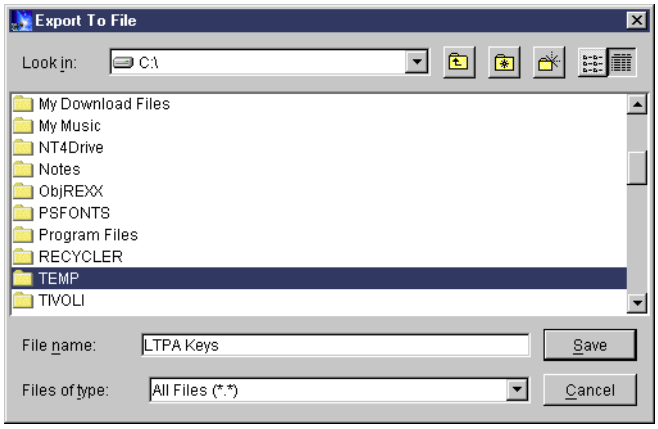

Figure 123. Exporting LTPA keys to a file

__ 14. Click **Save** to save the file.

__ 15. Click **Cancel** to close the Global Security Settings wizard.

Task 3: Creating a Directory Assistance Domino database

For Domino to use the OS/400 LDAP server, instead of its own LDAP, you must create a Directory Assistance database that points to the OS/400 LDAP server. To create a Directory Assistance database in Domino, perform the following steps:

__ 1. From your Lotus Notes client pull-down menu, select **File->Database->New**.

__ 2. From the New Database window, enter the following values (see Figure 124):

- Server = `DOMWASxx`
- Title = `Directory Assistance`
- File Name = `Director.nsf`

__ 3. Click the **Template Server** button, and select the **DOMWASxx** server.

__ 4. Select the **Directory Assistance** template (DA50.NTF).

__ 5. Make sure “Inherit future design changes” is selected, and click **OK**.

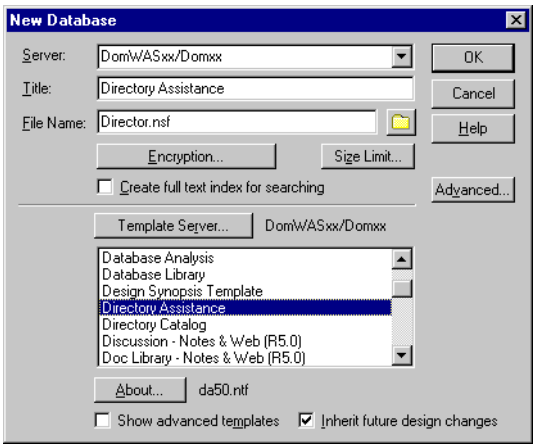

Figure 124. Create Directory Assistance database

__ 6. When the **Directory Assistance About** document appears, press Esc.

__ 7. You are now in the Directory Assistance database. Click the **Add Directory Assistance** button (Figure 125).

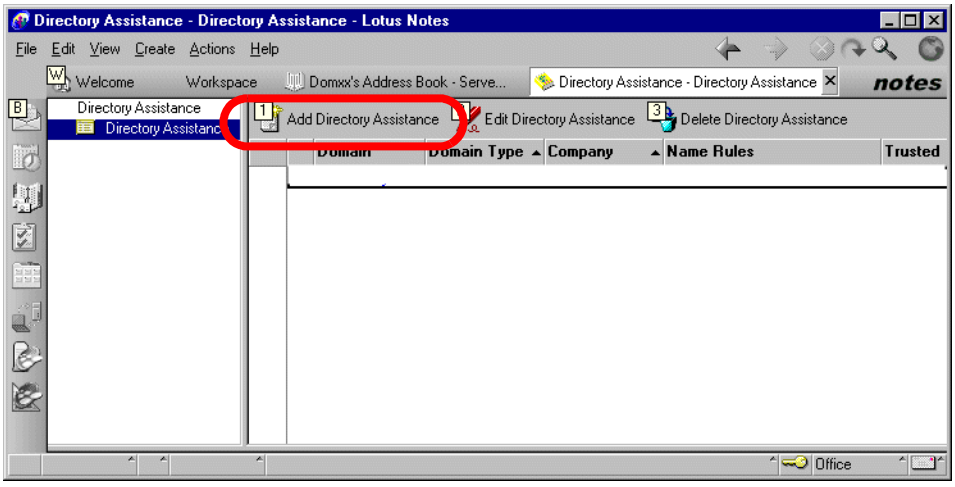

Figure 125. Domino Directory Assistance database

__ 8. Click the **Basics** tab and fill in the fields with the following values (Figure 126):

- Domain type: `LDAP`
- Domain name: `SecureWay`
- Company name: `IBM`

- Search order: Leave this field blank
- Group expansion: `Yes`
- Nested group expansion: `Yes`
- Enabled: `Yes`

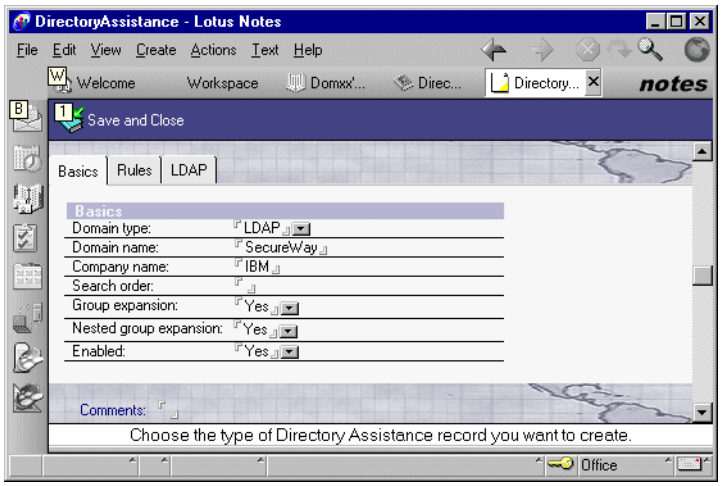

Figure 126. Directory Assistance: Basics tab

__ 9. Click the **Rules** tab and fill in the fields with the following values (Figure 127):

- For Rule 1, ensure that Enable is set to **Yes**
- For Rule 1, ensure that Trusted for Credentials is set to **Yes**

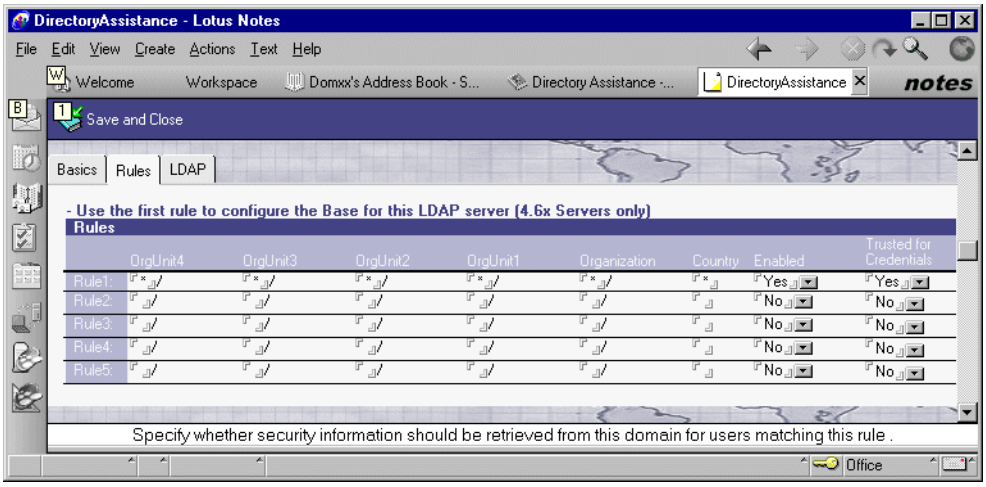

Figure 127. Directory Assistance: Rules tab

__ 10. Click the **LDAP** tab and fill in the fields with the following values (Figure 128 on page 100):

- Hostname: `PWDI.PID.IBM.COM`
- Optional Authentication Credentials Username: `cn=Administrator`
- Optional Authentication Credentials Password: `ldappw`
- Base DN for search: `ou=ITSO,o=IBM,c=US`
- Perform LDAP search for: `NotesClients/WebAuthentication`
- Channel encryption: `None`
- Leave all other fields as default

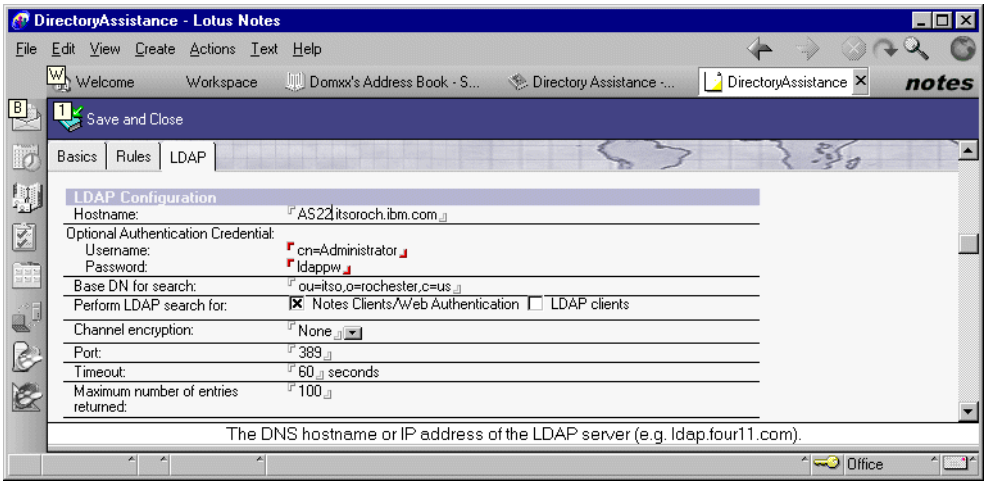

Figure 128. Directory Assistance: LDAP tab

__ 11. Click **Save and Close** to exit and save this document.

Task 4: Changing the Domino Server to use OS/400 LDAP

To change the Domino Server to use OS/400 LDAP, you must update the Domino server document and the Domino Web SSO document.

__ 1. From your Lotus Notes client, open the Domino Directory, and click the **Server** twistie. Click the **Servers** view (Figure 129).

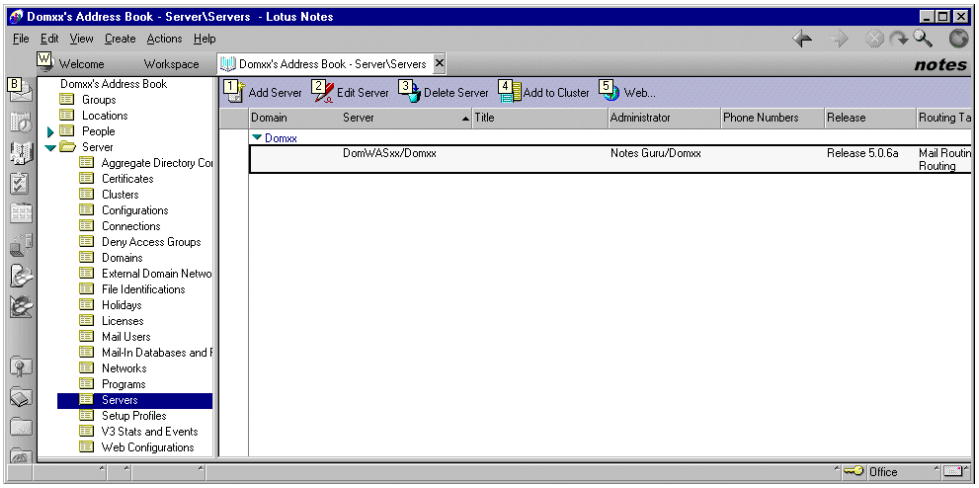

Figure 129. Domino server view

__ 2. Select your Domino server, and click the **Edit Server** button.

__ 3. Click the **Basic** tab. In the Directory Assistance database name field, type the filename `Director.nsf` (Figure 130).

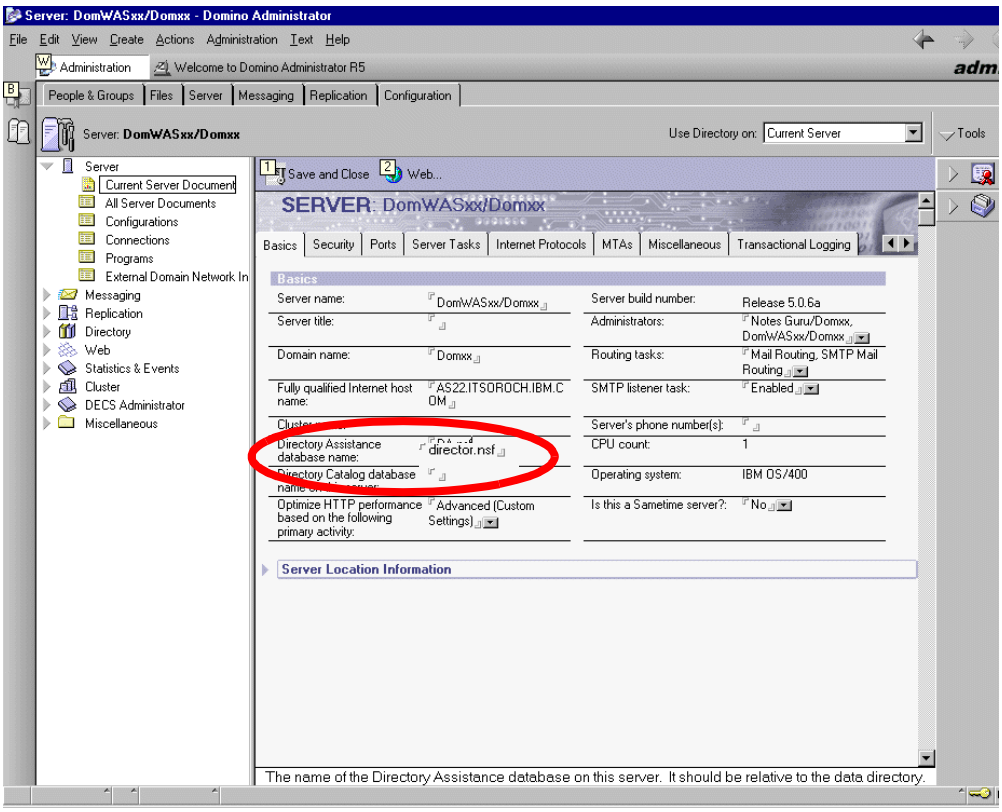

Figure 130. Adding the Directory Assistance database name to the Domino server

__ 4. Select the **Ports** tab, and then select the **Internet Ports** sub-tab. Then, select the **Directory** sub-sub-tab (Figure 131).

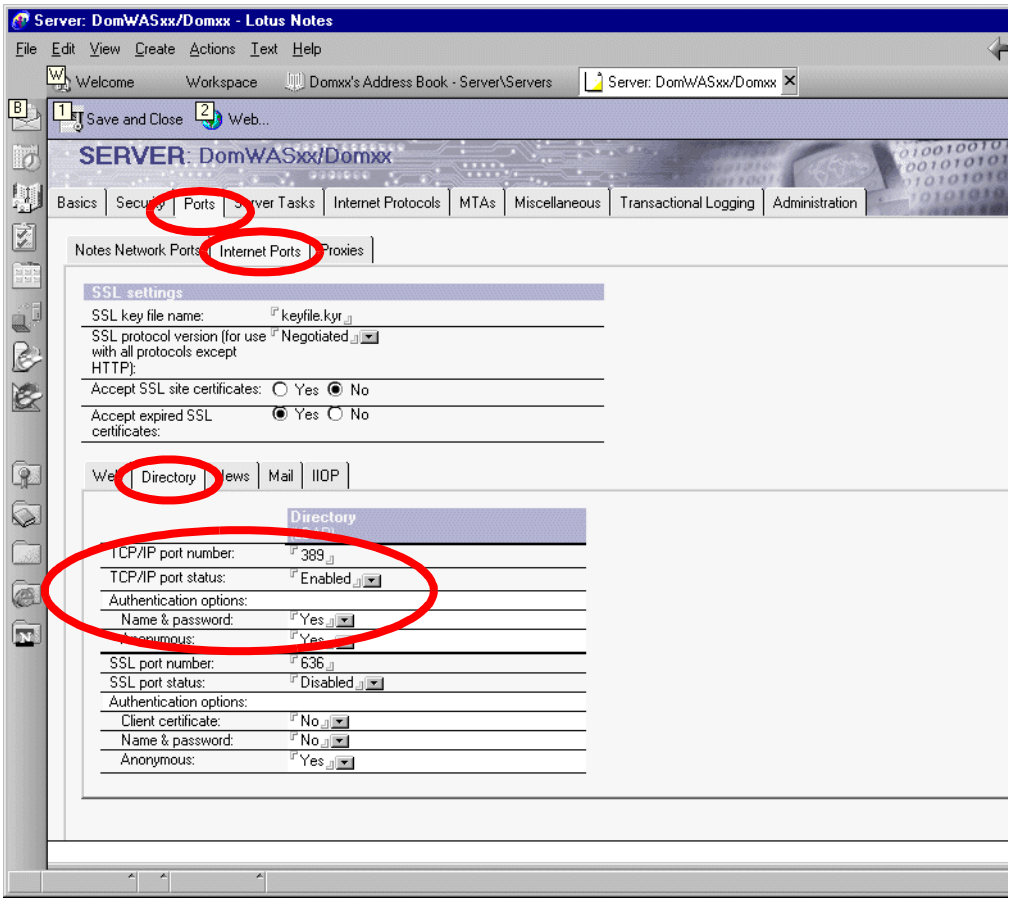

Figure 131. Changing the Directory port

__ 5. Change the TCP/IP port number to `389` and ensure that the Name & Password field in the TCP/IP Authentication options is set to `Yes` (Figure 131).

__ 6. Click the **Save and Close** button to save and exit the Domino Server document.

__ 7. From the Domino Directory database, select the **Web Configurations** view.

__ 8. Select your Web SSO Configuration document, and click the **Edit Document** button to edit the Web SSO Configuration for LtpaToken. It currently has the information from the old keys from when you were using the Domino LDAP server (Figure 132).

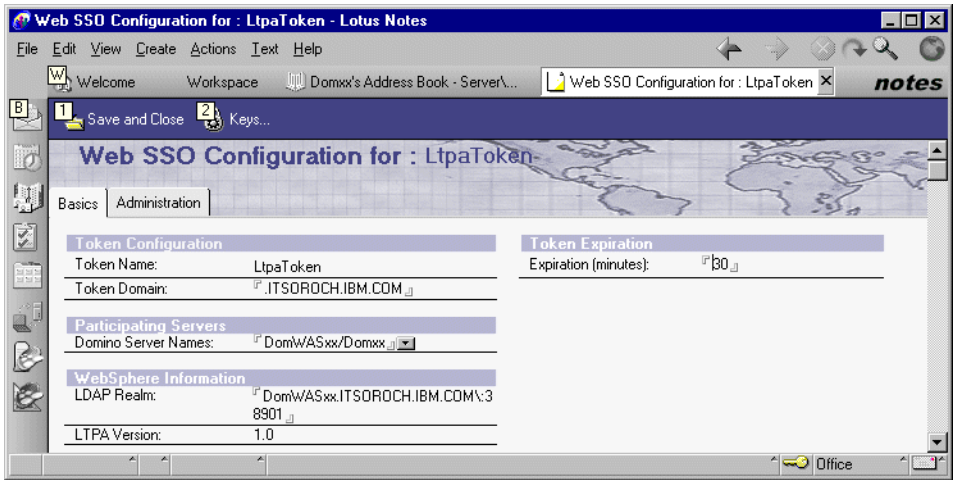

Figure 132. Web SSO Configuration document: Old LTPA Keys information

__ 9. You now import the new LTPA keys. Click the **Keys...** pull-down menu (shown in Figure 133), and select **Import WebSphere LTPA Keys**.

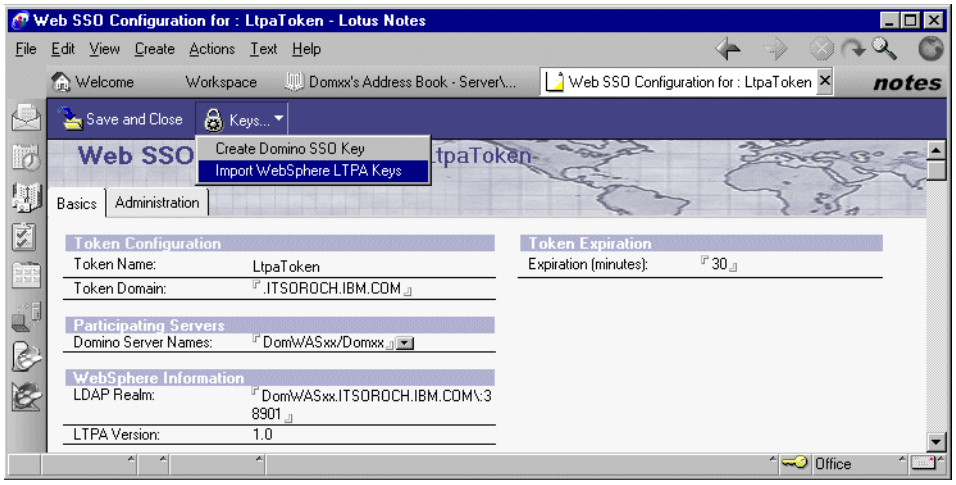

Figure 133. Selecting Import LPTA Keys from the Keys Pull-down menu

__ 10. On the Enter Import File Name window, enter the path to the LTPA Keys file that was exported earlier in this lab. Enter `c:\temp\LTPA Keys` and click on **OK** (Figure 134).

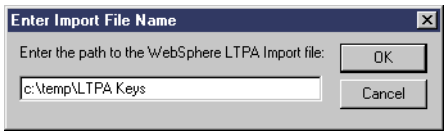

Figure 134. Entering the import file name for LTPA keys

__ 11. On the Enter Import File Password window, enter the password that you used earlier (dom2was) when generating the LTPA Keys (Figure 135). Click **OK**.

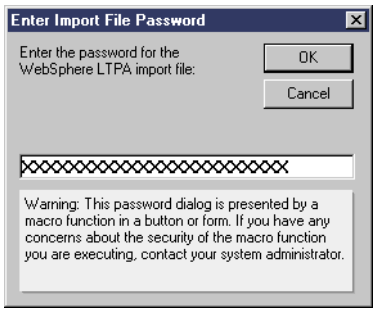

Figure 135. Entering the LTPA keys password

__ 12. On the Successfully imported WebSphere LTPA key window, click **OK** (Figure 136).

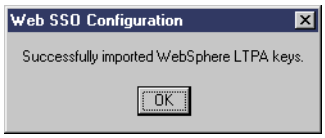

Figure 136. Import of LTPA keys successful

__ 13. The Web SSO Configuration document should automatically update to reflect the information from the LTPA Keys file you just imported.

__ 14. Figure 137 shows the Web SSO Configuration document with the following updated fields:

- **Token Expiration = <leave default>**

  This is the number of minutes a token can exist before expiring. A token does not expire based on inactivity. Rather, it is valid for only the number of minutes specified from the time of issue.

- **Token Domain = .PID.IBM.COM**

  This is the DNS domain portion of the fully qualified Internet name of your system. Since all servers participating in SSO must be in the same DNS domain, this value must be the same as the Domain value specified when configuring the WebSphere Application Server.

  Note: WebSphere Application Server treats the DNS domain as case-sensitive. Therefore, ensure that the DNS domain value is specified exactly the same (including case) whenever you use the value.

- **Domino Server Names = DOMWASxx/Domxx**

  These are the Domino servers that participate in SSO.

  Note: You must specify a fully qualified Domino server name here (for example, MyDominoServer/MyOu).

- **LDAP Realm = PWDI.PID.IBM.COM**

  This is the fully qualified host name of the LDAP server. This field is initialized from the information provided in the LTPA keys file.

Note: You only need to change this value if an LDAP server port value is specified for the WebSphere administrative domain. If a port is specified, a backslash (\) must be inserted in the value before the colon. For example, replace `mymachine.mydomain.ibm.com:389` with `mymachine.mydomain.ibm.com\:389`.

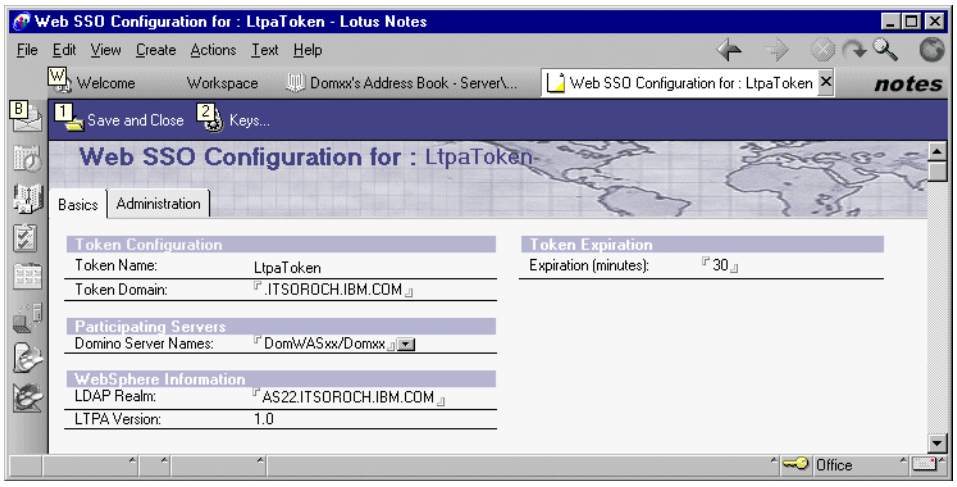

Figure 137. Updated Domino Web SSO Configuration document

__ 15. Click the **Save and close** button to save and exit the Web SSO Configuration document. Press Esc to exit the Domino Directory.

__ 16. You now add the DOMWASxx user profile to the ACL of the Domino WebSphere Lab (DomWASLab.nsf) database. From your Lotus Notes client workspace, right-click the Domino WebSphere Lab (**DomWASLab.nsf**) database icon and select **Database->Access Control**.

__ 17. In the Access Control window, select the entry for Notes Guru by single clickng it.

__ 18. Click the **Add** button to add a new user to the database ACL. On the Add User window, enter the following information and click **OK** (Figure 138):

`cn=DOMWASxx/ou=ITSO/o=IBM/c=US`

Note, the syntax here is different from the LDAP syntax because a slash (/) is used instead of the comma (,).

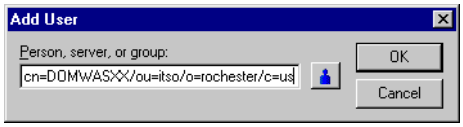

Figure 138. Adding a user in LDAP format

__ 19. When a user is added, the format appears different from what you entered, that is the hirachy identifiers (o=, ou=, c=) disappeared. This is expected. Make sure the new ACL member has Manager authority for the database (this should be accomplished by automatically, since you selected Notes Guru in step __ 17., on page 105 before adding the new entry. Click **OK** to exit the Access Control window (Figure 139).

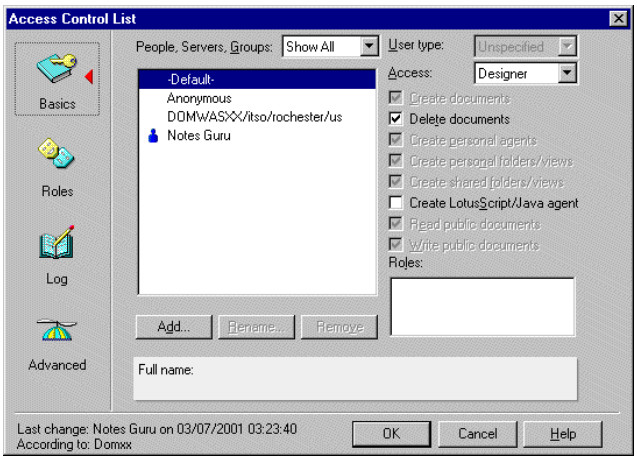

Figure 139. New OS/400 user added to ACL

__ 20. For these changes to take effect, the Domino server must be stopped and restarted. To do this, from your 5250 session, enter the following command and press **Enter**:

```
WRKDOMSVR DOMWASxx
```

__ 21. From the Work with Domino Servers screen, enter option `8` (Work Console) next to your Domino server.

__ 22. In the *Work with Domino Console* enter the following command:

```
restart server
```

__ 23. Press **F5** until you see the server restarted successfully.

__ 24. You now need to start your Domino HTTP server. From the Work with Domino Servers screen, enter option `8` (Work Console) to go into the Domino server console. Enter the `load http` command to start the Domino HTTP server task.

__ 25. Press F5 to refresh the screen and verify that the HTTP task starts successfully. Press F3 to exit the Domino console.

Task 5: Verifying Single Sign-On between Domino and WebSphere

You are now ready to verify that SSO for WebSphere and Domino is still configured and working correctly using OS/400 LDAP. This time, however, you enter your `DOMWASxx` OS/400 user ID.

You must first test opening the servlet in WebSphere and then link to the Domino application. You should only be prompted to sign on once when you initially go to the SimpleServlet. After that, you should be able to move back and forth between the two applications without being prompted to sign on.

Your next test is to go the Domino application and then link to the SimpleServlet in WebSphere. Again, you should only be prompted once when you initially go into the Domino application. After that, you should again be able to move back and forth between the two applications without being prompted to sign on.

SimpleServlet to Domino application SSO test

Perform the following tasks to test the SimpleServlet to Domino application SSO:

__ 1. Open your Netscape browser and enter the following URL:

`http://PWDI.PID.IBM.COM:80xx/webapp/DomApp/SimpleServlet`

You are prompted to sign on. Enter your user name (`DOMWASxx`) and password (`dom2was`) as shown in Figure 140. Click **OK**.

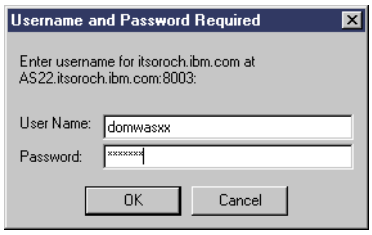

Figure 140. SimpleServlet sign on

__ 2. You are prompted to accept a cookie (Figure 141). This cookie is generated as a result of SSO. Click **OK**.

Figure 141. SSO cookie

__ 3. You are prompted to accept another cookie (Figure 142). This is the original cookie that appeared before enabling SSO. Click **OK**.

Figure 142. Cookie

__ 4. The SimpleServlet Web page appears (Figure 143 on page 108).

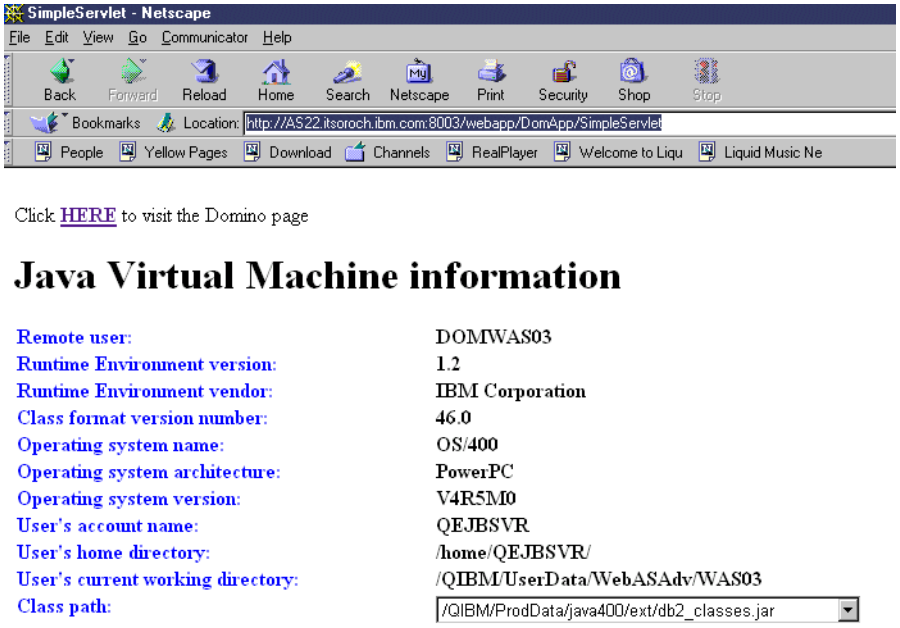

Figure 143. SimpleServlet

__ 5. To access the Domino application from the servlet, click the link:

```
Click HERE to visit the Domino page
```

Because you enabled the Single Sign-On ability between WebSphere and Domino, you should not be prompted by Domino to sign on again to access the Domino application. Rather, you should be taken directly into the Domino application (Figure 144).

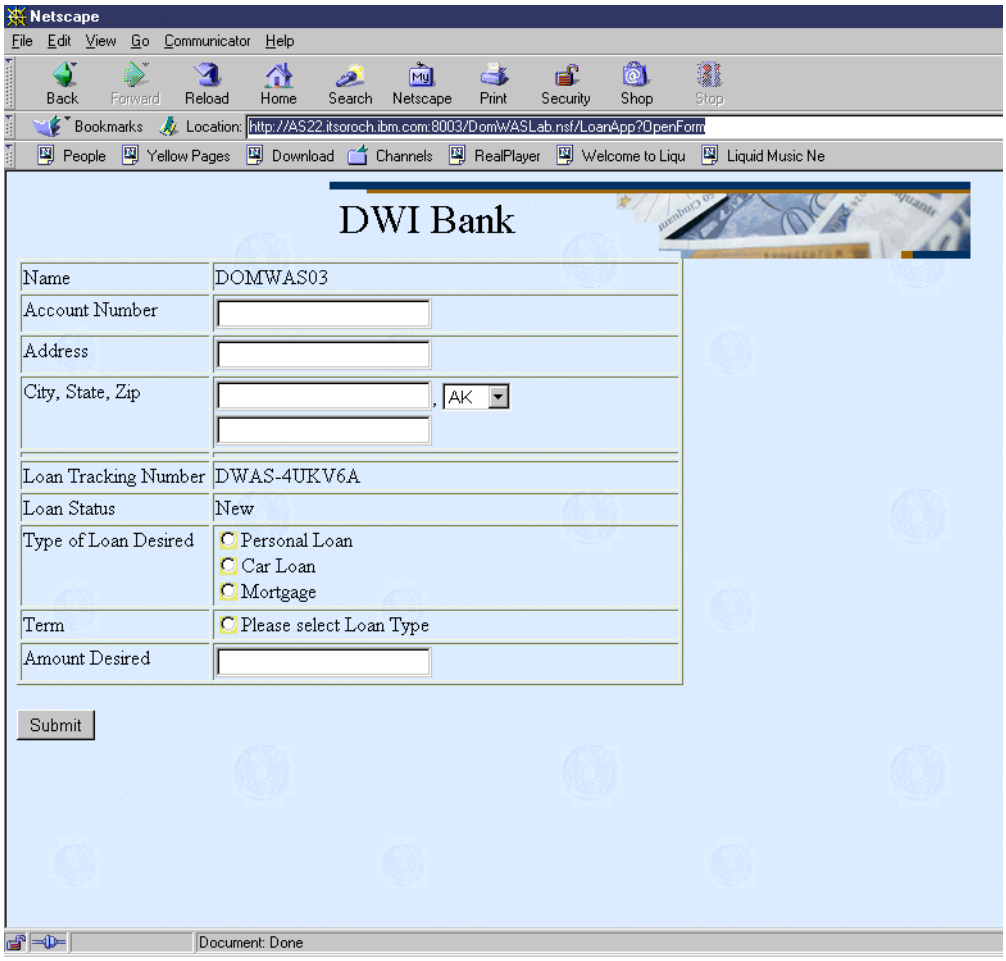

Figure 144. Domino application

Domino application to SimpleServlet SSO test

Perform the following the tasks to test the Domino application to SimpleServlet SSO:

__ 1. Close your Netscape browser window and re-open it to remove the cookies that were set in the previous test.

__ 2. From the Netscape browser, go to the DomWASLab.nsf Domino Web application by entering the following URL (remember to replace *xx* with your team number):

```
http://PWDI.PID.IBM.COM:80xx/DomWASLab.nsf/loanapp?openform
```

The Web page shown in Figure 145 on page 110 should appear and prompt you for a valid user name and password. Enter the user name (`DOMWASxx`) and password (`dom2was`). Click **Login**.

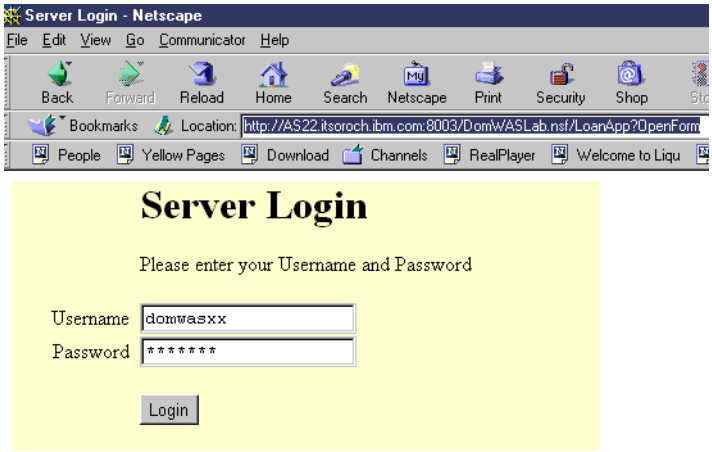

Figure 145. Domino SSO challenge

__ 3. You are prompted to accept a cookie (Figure 146). This cookie is generated as a result of SSO. Click **OK**.

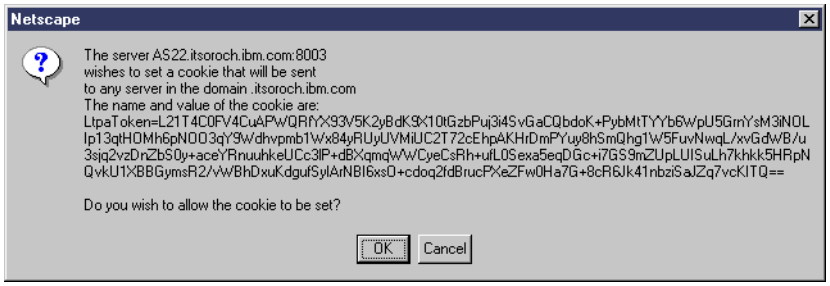

Figure 146. SSO cookie

__ 4. The Domino application window appears (Figure 147).

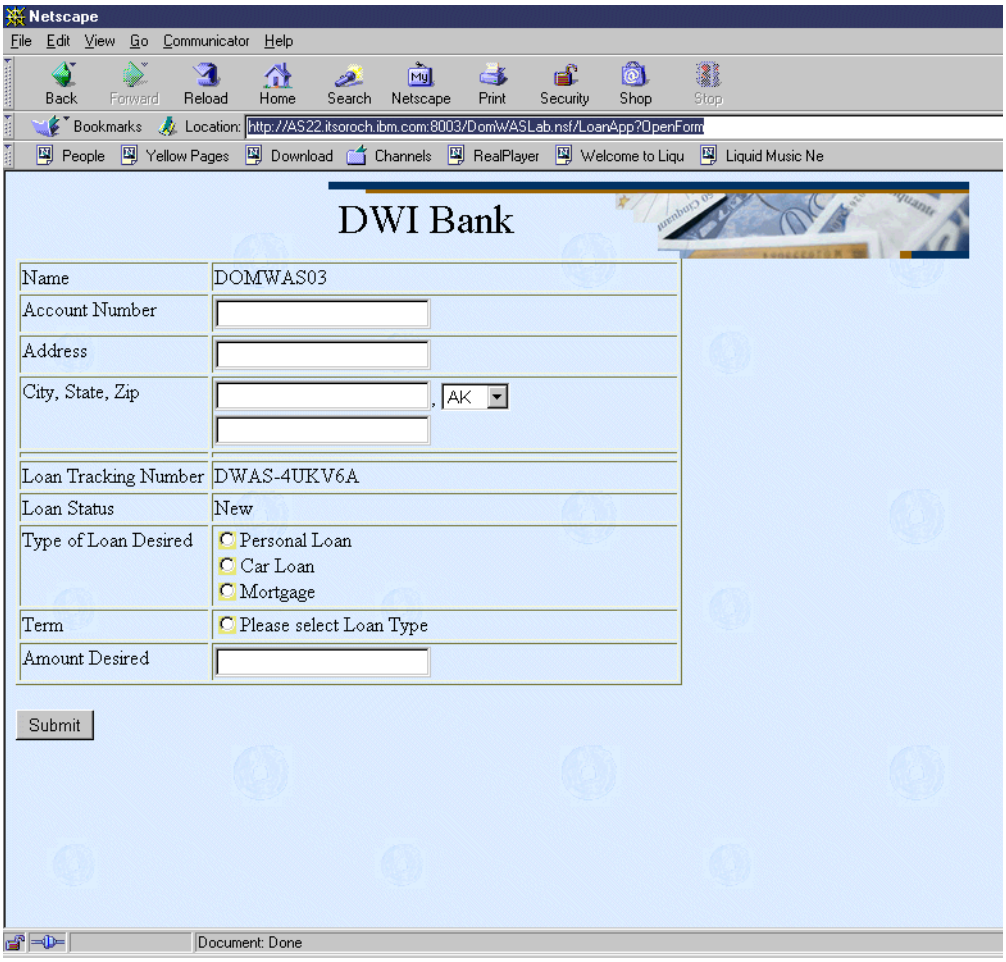

Figure 147. Domino loan application

__ 5. Click the **Submit** button to get to the link to the WebSphere SimpleServlet.

__ 6. On the next Web page that appears (Figure 148), click the link:

`Return to the Main Menu`

This will take you to the WebSphere SimpleServlet.

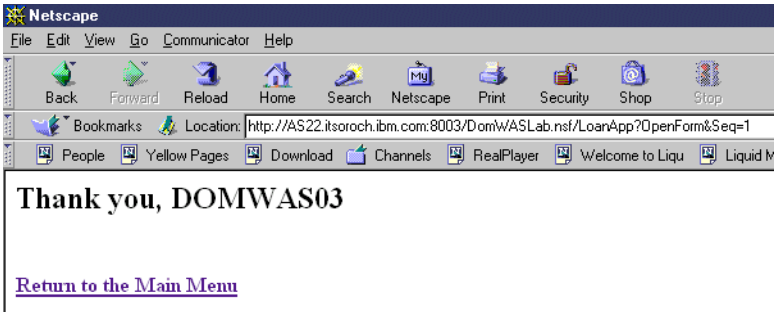

Figure 148. Domino application link to SimpleServlet

__ 7. You are prompted to accept another cookie (Figure 149). This is the original cookie that appeared before enabling SSO. Click **OK**.

Figure 149. Cookie

__ 8. Again, because you enabled the Single Sign-On ability between WebSphere and Domino, you should not be prompted by WebSphere to sign on again to access the SimpleServlet. The WebSphere SimpleServlet should appear (Figure 143 on page 108).

Lab 7. Optional lab: Using IBM HTTP Server for OS/400

During the previous lab exercises, you used Lotus Domino for AS/400 as your HTTP server. In this lab, you set up a WebSphere Application Server 3.5.2 instance and Domino server to use an instance of the IBM HTTP Server for OS/400. You then test your Single Sign-On environment again.

The Domino plug-in for OS/400 HTTP Server allows you to perform OS/400 HTTP Web serving of both Domino and non-Domino content using a single Web server. With this support, Domino can be set up to use the OS/400 HTTP Server instead of its own internal HTTP server. This results in simpler administration and a reduction in the number of required internet ports.

Objectives

This lab teaches you how to:

- Change the HTTP configuration of your Domino server to use OS/400 HTTP.
- Create an instance of the IBM HTTP Server for OS/400.
- Reconfigure the OS/400 HTTP Server to support Domino.
- Restart your Domino and WebSphere Single Sign-On environment using OS/400 HTTP.

Important

Throughout these lab exercises, replace *xx* with your team number. Also, refer to Table 1 on page 4 to make sure the correct values for the configuration parameters are entered.

Task 1: Changing the HTTP configuration on your Domino Server

Before making the switch to using the OS/400 HTTP stack, you must change the HTTP configuration of your Domino Server. To do this, you delete the configuration you created in Task 2 of Lab 1. “Developing a Domino application” on page 9.

Modifying the Domino Server document

Perform the following tasks to modify the Domino Server document:

__ 1. From your Lotus Notes client, open the Domino Directory on the Domino server for your team (DOMWASxx).

__ 2. Expand the **Server** folder and open the **Servers** view.

__ 3. Select the Domino server document for your Domino server (DOMWASxx) and click the **Edit** button.

__ 4. In the Domino Server document, select the **Internet Protocols** tab, and then select the **HTTP** tab.

__ 5. In the middle of the right column, in the DSAPI filter file names field, delete the following file name:

```
/qsys.lib/qejb.lib/domino.srvpgm
```

__ 6. Click **Save and Close** to save and exit the Domino server document.

Modifying the Domino server notes.ini file

Perform the following tasks to modify the Domino server notes.ini file:

__ 1. From your 5250 emulation session, enter the following command on the OS/400 command line and press Enter:

```
wrkdomsvr
```

__ 2. From the Work with Domino Servers display, enter option `13` (Edit NOTES.INI) in the Opt field next to your Domino server (DOMWASxx) and press Enter.

__ 3. From the Edit File display, scroll down until you find the following statement and delete it by placing a `d` next to that line and press Enter:

```
WebSphereInit=/qibm/UserData/WebASAdv/WASxx/properties/
bootstrap.properties
```

__ 4. Press F3 twice to save and exit the notes.ini file.

__ 5. To end the Domino server, from the Work with Domino Server display, enter option `6` (End Server) in the Opt field next to *your* Domino server (DOMWASxx) and press Enter. This ends the Domino server until you create your instance of the IBM HTTP Server for OS/400.

Task 2: Creating an instance of the IBM HTTP Server for OS/400

Because each student team uses a separate instance of the WebSphere Application Server 3.5.2, with its own unique HTTP port, you also need to set up a unique instance of the IBM HTTP Server for OS/400.

Creating the HTTP server configuration and instance

Perform the following tasks to create the HTTP server configuration and instance:

__ 1. To create your HTTP server configuration and instance, you must access the HTTP Administrative server on the AS/400 or iSeries server. This is a special server instance capable of allowing administrators to modify server configurations as well as start, stop, and restart instances of the HTTP server remotely over the Web.

__ 2. By default, the HTTP Administrative server runs on port 2001. Start your Netscape browser and enter the following URL:

```
http://PWDI:2001
```

Here, *PWDI* is the hostname of the classroom iSeries server. Enter your OS/400 user ID and password information when prompted. The window shown in Figure 150 should appear.

Figure 150. AS/400 Tasks

__ 3. Click **IBM HTTP Server for AS/400**.

__ 4. On the IBM HTTP Server for AS/400 Web page, click the **Configuration and Administration** link (Figure 151).

Figure 151. IBM HTTP Server for AS/400 Web page

__ 5. You must now create a configuration for your new HTTP server instance. From the Configuration and Administration Web page, on the navigation frame on the left side of the window, select **Configurations->Create configuration**.

__ 6. The right frame prompts you for a configuration name, which can be anything. However, for the purposes of this lab, use your OS/400 user ID (`DomWASxx`).

Leave the Create Empty Config radio button selected, and click **Apply** (see Figure 152).

> **Attention**
>
> Remember to click **Apply** whenever you make changes in this environment or the changes will not be saved.

Figure 152. Create HTTP configuration

__ 7. A message appears indicating that the HTTP server configuration file was successfully created.

__ 8. Select the name of your HTTP configuration from the drop-down box in the left navigation frame, and click **Basic**. Enter the following values (Figure 153):

- Host Name = `PWDI`
- Default port = `80xx` (where *xx* is your team number)

Be sure to click **Apply** so the changes take effect.

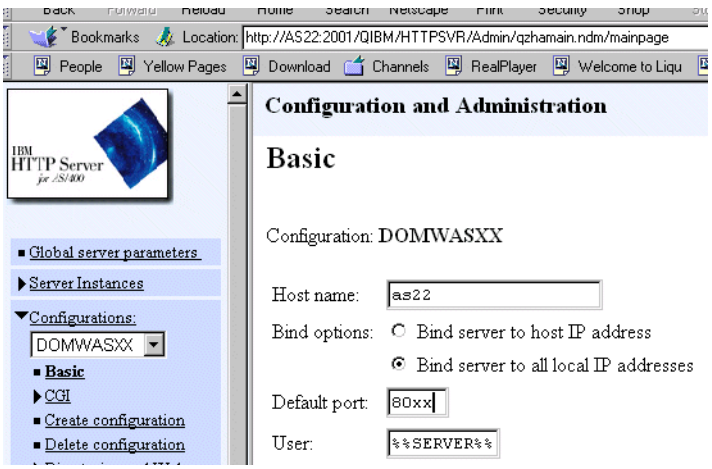

Figure 153. HTTP server Basic configuration

__ 9. You should receive the following message:

```
"The configuration file was successfully updated. Server instances that
are using this configuration must be stopped and started for the changes
to take affect."
```

__ 10. You must now enable the required HTTP methods. This allows the HTTP server to process CGI (then pass it to WebSphere). Click **Request Processing** in the left navigation frame, and then click **Methods**. Select the **Get** and **Post** boxes. You may leave the other methods as the default. Click **Apply**. The following message should appear:

```
"The configuration file was successfully updated. Server instances that
are using this configuration must be stopped and started for the changes
to take affect."
```

__ 11. Add support for Java servlets and JSPs by clicking the **Java Servlets** link in the left navigation frame. On the Java Servlets Configuration and Administration Web page, select the **WebSphere version 3** radio button (Figure 154).

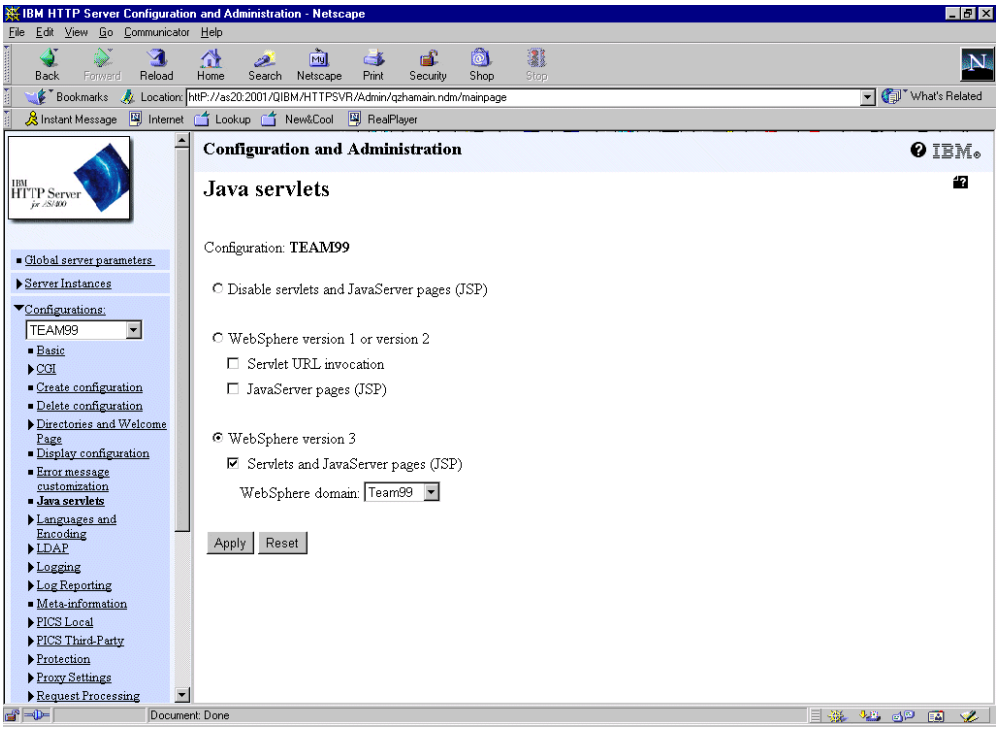

Figure 154. Java servlets Web page

__ 12. Select your WebSphere domain configuration (**WASxx**) from the drop-down box. Click **Apply** to add the WebSphere version 3 routing entries to your HTTP configuration file. The following message should appear:

```
"The configuration file was successfully updated. Server instances that
are using this configuration must be restarted for the changes to take
affect. Go to the Application Server Manager to do additional
configuration."
```

__ 13. You now add a routing entry for serving HTML files and applets. Click the **Request Routing** link in the left navigation frame.

On the Request Routing Web page select an **Index** number and then select either **Insert before** or **Insert after**.

Fill in the appropriate fields with the values listed in Table 2, and then click **Apply** (Figure 155).

Table 2. Request Routing Web page field values

Action	URL Template	Replacement file path
Pass	/html/*	/QIBM/UserData/WebASAdv/WASxx/html/*

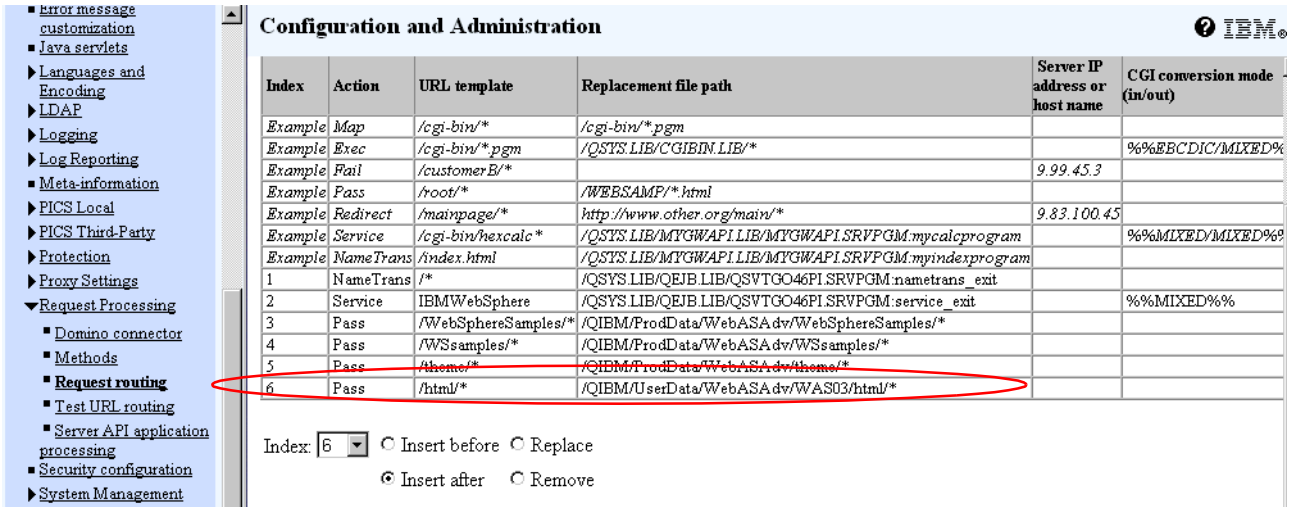

Figure 155. Request Routing Web page

The following message should appear:

```
"The configuration file was successfully updated. Server instances that
are using this configuration must be restarted for the changes to take
affect."
```

__ 14. You must create an HTTP server instance to use this HTTP configuration. Click **Server instances** in the left navigation pane, and then click **Create server instance**. Name your HTTP instance `WASxx`. Select your HTTP configuration (**DOMWASxx**) from the drop-down box and click **Create**. The following message should appear:

```
"The server instance was successfully created."
```

__ 15. Start the OS/400 HTTP server by clicking **Work with server instances** from the left navigation pane. Select your server instance (**WASxx**), and click **Start**. The following message should appear:

```
"The server instance was successfully started."
```

Task 3: Testing your OS/400 HTTP configuration

Now that the HTTP server instance is configured and started, you may test it by running the “Snoop” servlet.

__ 1. From your Netscape browser, run the Snoop servlet by entering the following URL:

```
http://AS22.itsoroch.ibm.com:8003/servlet/snoop
```

The Web page shown in Figure 156 should appear.

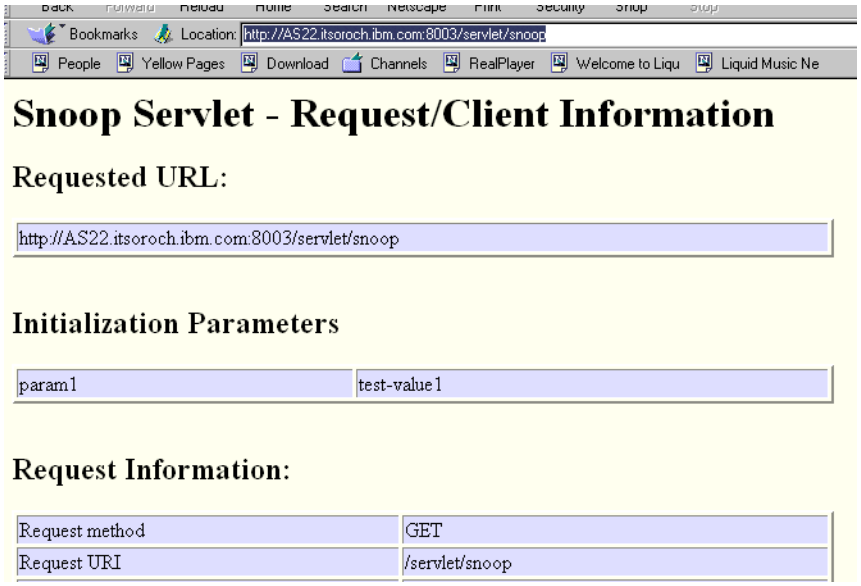

Figure 156. Snoop servlet

Task 4: Reconfiguring the OS/400 HTTP Server for Domino

In this task, you add more configuration information to the HTTP instance you set up in the previous lab to enable the Domino plug-in for the OS/400 HTTP Server.

__ 1. From your Netscape browser, go back to the Administrative server by entering the following URL:

```
http://PWDI:2001
```

Here, *PWDI* is the hostname of the classroom iSeries server. If you are prompted, enter your OS/400 user ID and password information. The Web page shown in Figure 157 should appear.

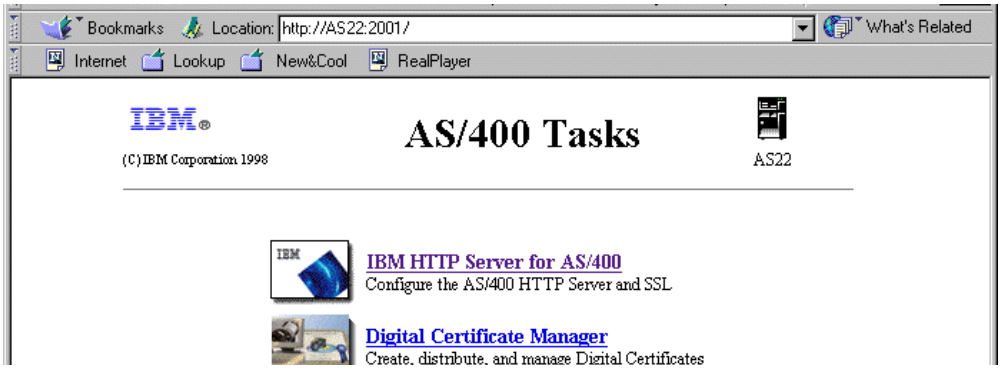

Figure 157. AS/400 Tasks

__ 2. Click **IBM HTTP Server for AS/400**. On the Web page that appears, click **Configuration and Administration**.

__ 3. From the IBM HTTP Server Configuration and Administration Web page, end the OS/400 HTTP server by clicking **Server Instances**. Click **Work with server instances** from the left navigation pane.

__ 4. Select your server instance (**WASxx**), and click **Stop**. The following message should appear:

```
"The server instance was successfully stopped."
```

__ 5. Click **Configurations** in the left navigation pane and then select the configuration you created (**DOMWASxx**) from the drop-down list.

__ 6. Add a routing entry for serving Domino files by clicking **Request Processing**.

__ 7. Then, click **Request Routing**. Add the three lines shown in Table 3.

Click **Apply** so the changes take effect as shown in Figure 158.

Table 3. Request Routing field values for Domino support

Action	URL template	Replacement file path	CGI conversion mode (in/out)
Service	`*.nsf*`	`/QSYS.LIB/QNOTES.LIB/LIBHTTPX.SRVPGM:Service`	`%%BINARY/MIXED%%`
Pass	`/icons/*`	`/DomWASLab/xx/domino/icons/*`	
Pass	`/domjava/*`	`/DomWASLab/xx/domino/JAVA/*`	

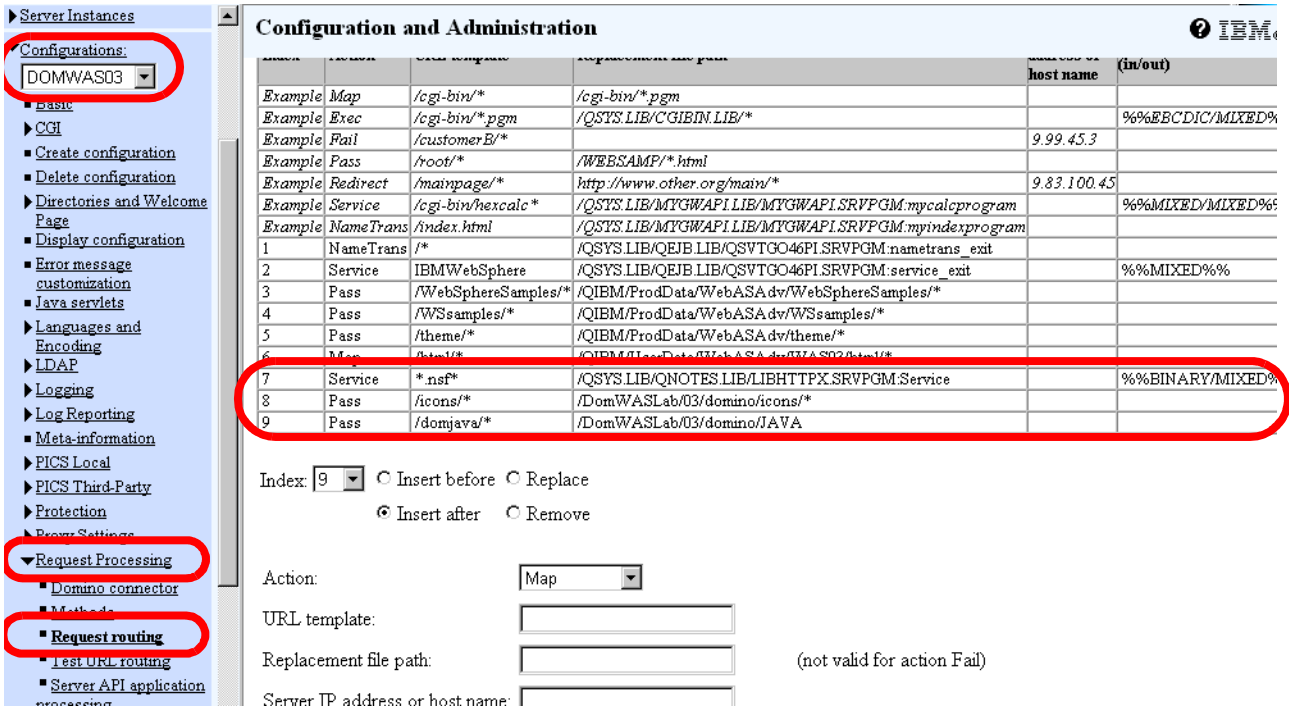

Figure 158. Request routing settings

__ 8. Specify the Domino plug-in for your OS/400 HTTP Server. Click **Server API Application Processing** from the left navigation pane and add the two field values shown in Table 4.

Click **Apply** so the changes can take effect as shown in Figure 159.

Table 4. Field values for Server API Application Processing

Step	Application path and file name
ServerInit	/QSYS.LIB/QNOTES.LIB/LIBHTTPX.SRVPGM:ServerInit
ServerTerm	/QSYS.LIB/QNOTES.LIB/LIBHTTPX.SRVPGM:ServerTerm

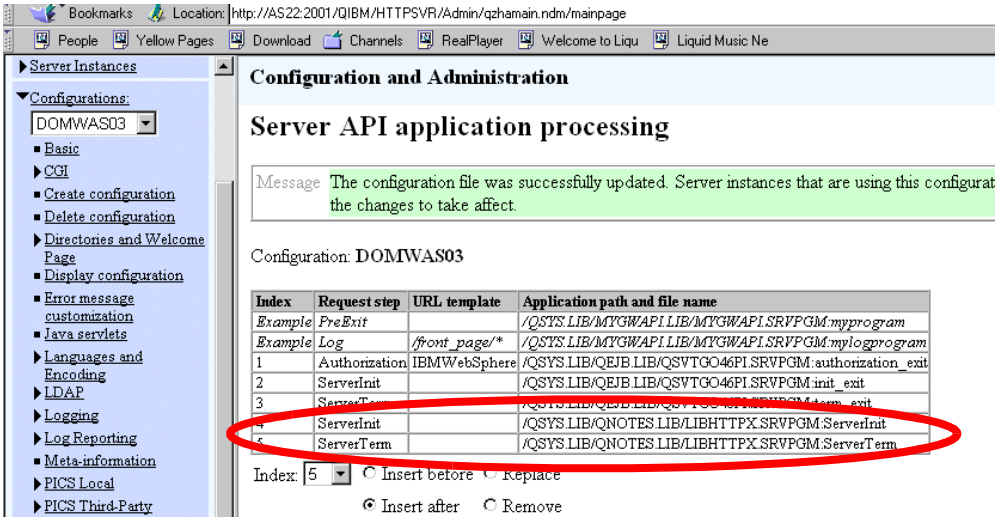

Figure 159. Server API Application Processing settings

__ 9. Before restarting your OS/400 HTTP server instance with the changes you just made, you must change the configuration of your Domino server to use this OS/400 HTTP instance to provide Web service for Domino. From a 5250 emulation window, enter the following command:

```
CHGDOMSVR SERVER(DOMWASxx) WEB(WASxx)     (where xx = your team number)
```

(You may also use option 2 in the *Work with Domino Servers* panel)

__ 10. Start your Domino Server using the following OS/400 CL command:

```
STRDOMSVR SERVER(DOMWASxx)     (where xx = your team number)
```

(You may also use option 1 in the *Work with Domino Servers* panel)

Note: We recommend that you always start the Domino server before starting the OS/400 HTTP server. Similarly, you should always end the OS/400 HTTP server before ending the Domino server.

__ 11. On your Netscape browser window, click **Server Instances** from the top of the left navigation pane, and then click **Work with server instances**. Select your HTTP server instance (**WASxx**), and click the **Start** button to start your HTTP server instance again. The following message should appear:

```
"The server instance was successfully started."
```

Task 5: Verifying Single Sign-On between Domino and WebSphere

At this point, you are ready to verify that SSO for WebSphere and Domino is still configured and working correctly using OS/400 HTTP.

You should test going to the servlet in WebSphere and then linking to the Domino application. You should only be prompted to sign on once when you initially go to the SimpleServlet. You should then be able to move back and forth between the two applications without being prompted to sign on.

The second test is to go the Domino application and then link to the SimpleServlet in WebSphere. Again, you should only be prompted once when you initially go into the Domino application. After that, you should be able to move back and forth between the two applications without being prompted to sign on.

SimpleServlet to Domino application SSO test

Perform the following tasks to test your SimpleServlet to Domino application SSO:

__ 1. Open your Netscape browser and enter the following URL:

`http://PWDI.PID.IBM.COM:80xx/webapp/DomApp/SimpleServlet`

You are prompted to sign on. Enter your user name (`DOMWASxx`) and password (`dom2was`) (Figure 160). Click **OK**.

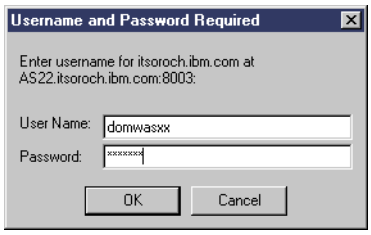

Figure 160. SimpleServlet sign on

__ 2. You are prompted to accept a cookie (Figure 161). This cookie is generated as a result of SSO. Click **OK**.

Figure 161. SSO cookie

__ 3. You are prompted to accept another cookie (Figure 162). This is the original cookie that you saw before enabling SSO. Click **OK**.

Figure 162. Cookie

__ 4. The SimpleServlet Web page appears (Figure 163).

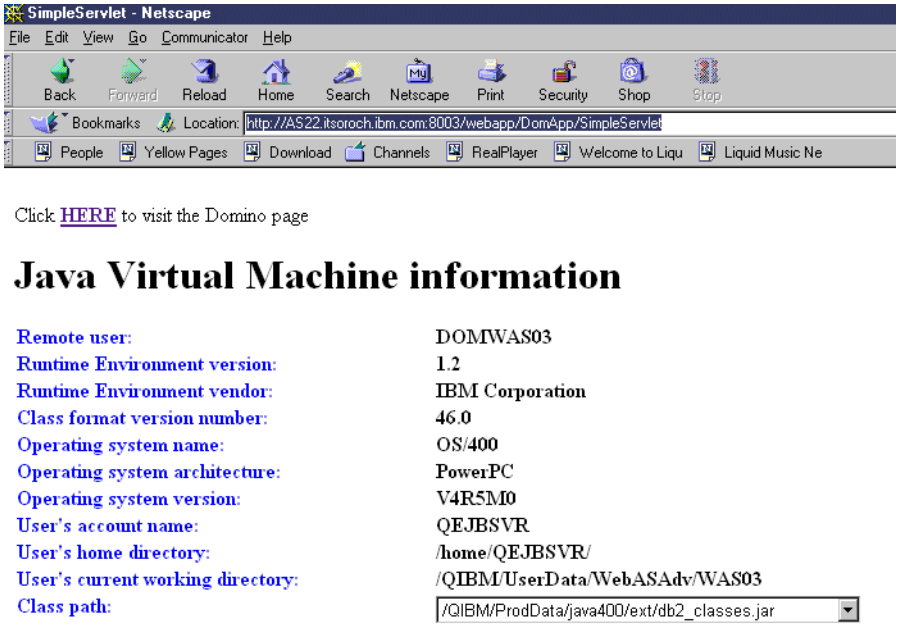

Figure 163. SimpleServlet Web page

__ 5. To access the Domino application from the servlet, click the link:

```
Click HERE to visit the Domino page
```

Since you have enabled the Single Sign-On ability between WebSphere and Domino, you are not prompted by Domino to sign on again to access the Domino application. Rather, you are taken directly into the Domino application (Figure 164).

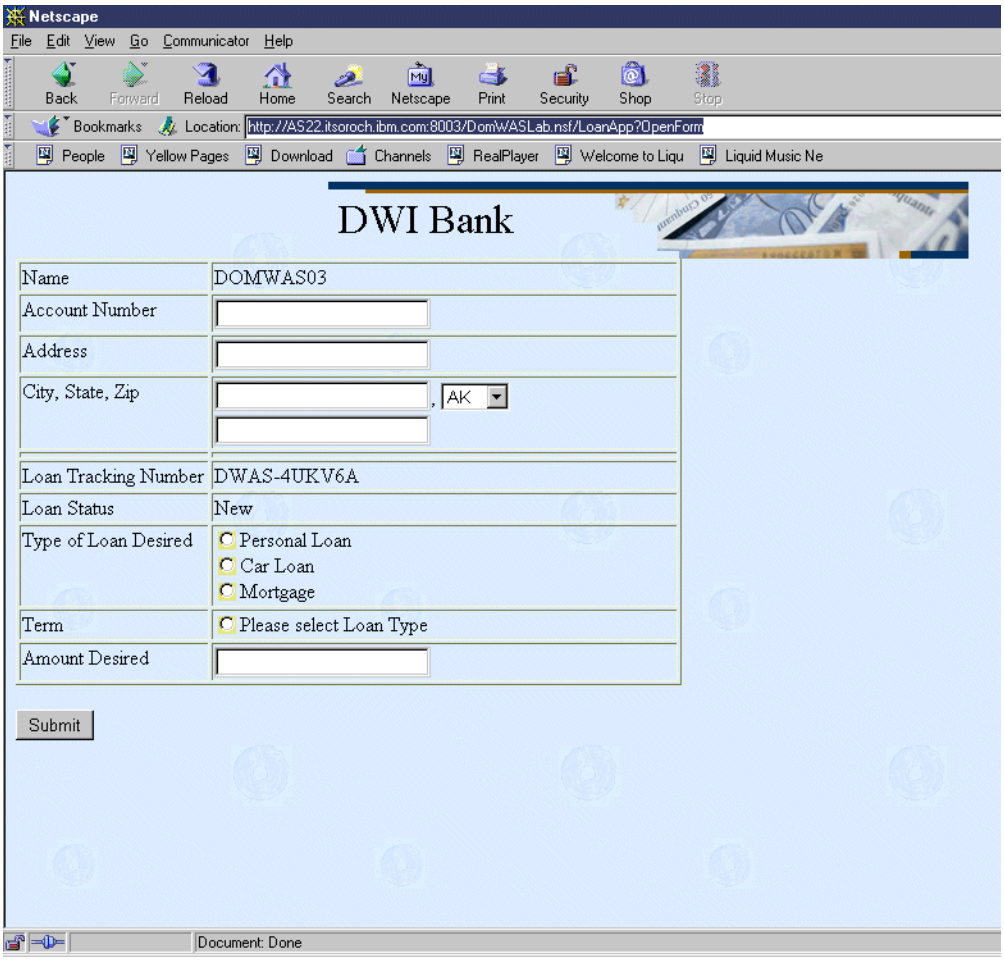

Figure 164. Domino application

Domino application to SimpleServlet SSO test

Perform the following tasks to test your Domino application to SimpleServlet SSO:

__ 1. Close your Netscape browser window and re-open it to remove the cookies that were set in the previous test.

__ 2. From the Netscape browser, go to the Domino Web application (DomWASLab.nsf) by entering the following URL (remember to replace *xx* with your team number):

```
http://PWDI.PID.IBM.COM:80xx/DomWASLab.nsf/loanapp?openform
```

The Web page shown in Figure 165 on page 125 appears asking for a valid user name and password. Enter the user name (`DOMWASxx`) and password (`dom2was`), and click **Login**.

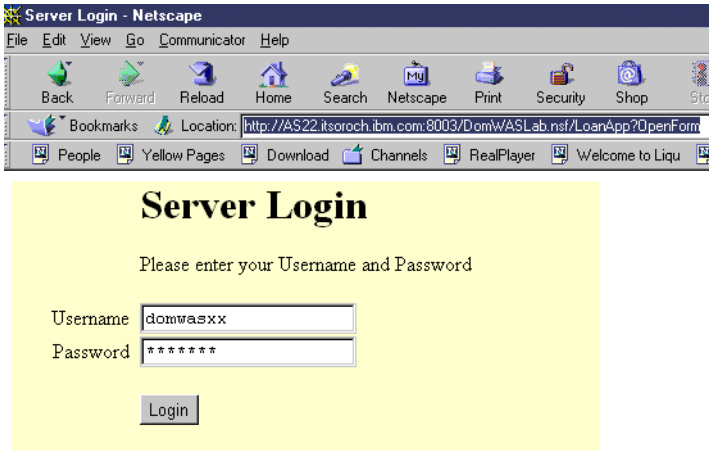

Figure 165. Domino SSO challenge

__ 3. You are prompted to accept a cookie (Figure 166). This cookie is generated as a result of SSO. Click **OK**.

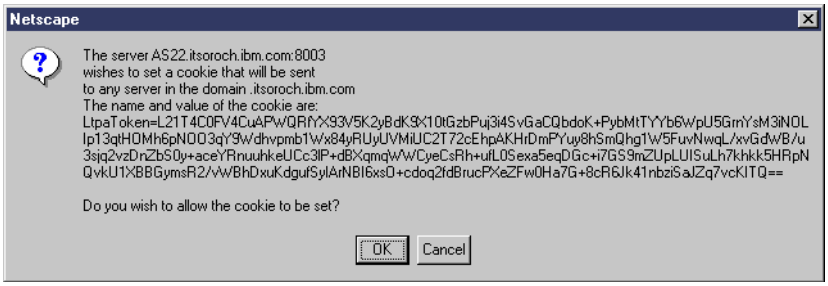

Figure 166. SSO cookie

__ 4. The Domino application appears (Figure 167).

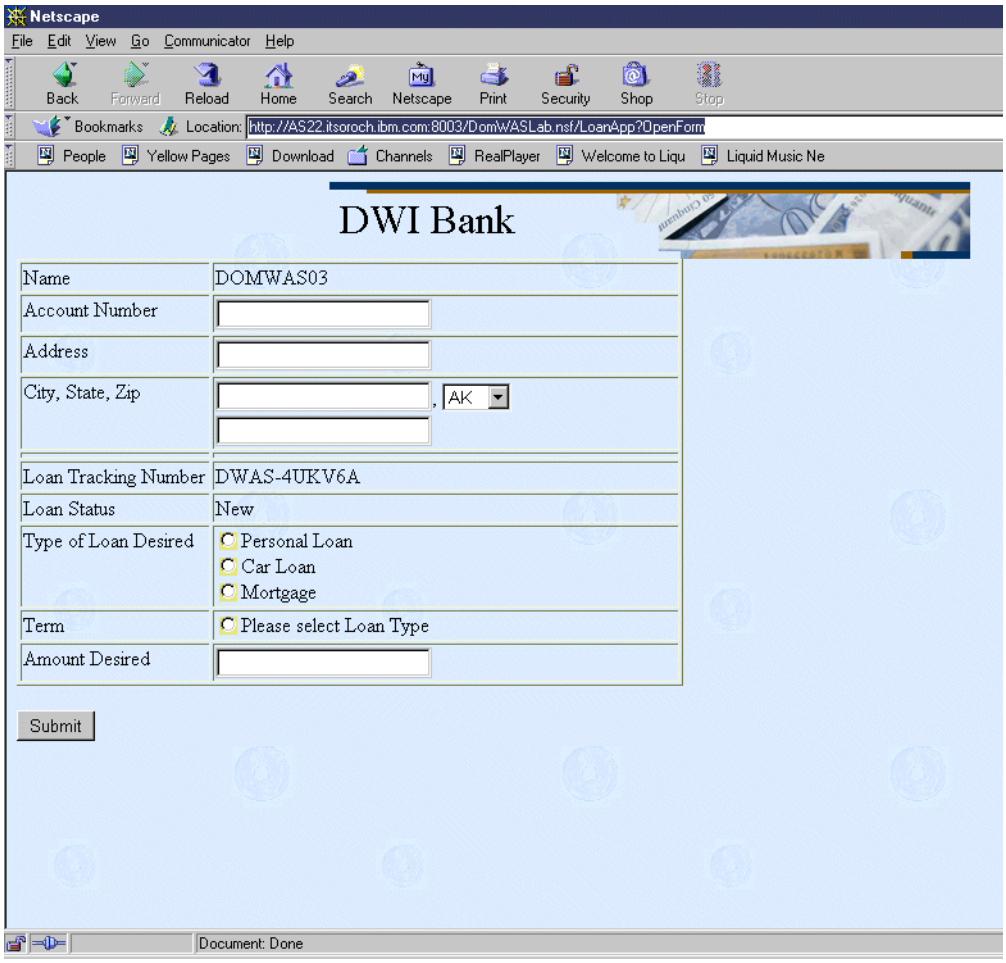

Figure 167. Domino loan application

__ 5. Click the **Submit** button to get to the link to the WebSphere SimpleServlet.

__ 6. On the Web page that appears (Figure 168), click the link:

`Return to the Main Menu`

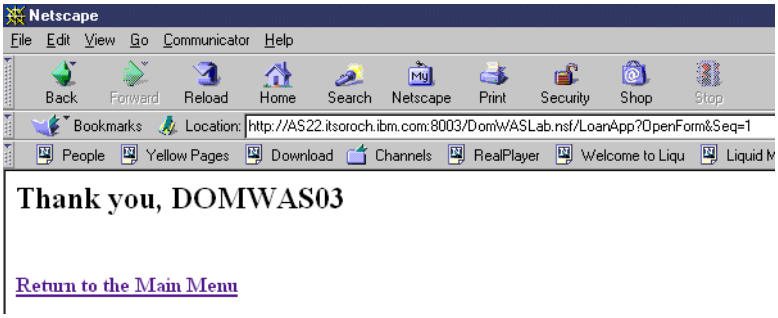

Figure 168. Domino application link to SimpleServlet

__ 7. You are prompted to accept another cookie (Figure 169). This is the original cookie that you saw before enabling SSO. Click **OK**.

Figure 169. Cookie

__ 8. Again, since you enabled the Single Sign-On ability between WebSphere and Domino, you are not prompted by WebSphere to sign on again to access the SimpleServlet. The WebSphere SimpleServlet appears (Figure 163 on page 123).

Lab 8. Information only: Configuring the OS/400 LDAP server

This lab is for informational purposes only. Do *not* perform the tasks shown in this lab. This lab explains how to configure OS/400 LDAP and then publish entries from the OS/400 System Distribution Directory to the LDAP directory.

Objectives

This lab teaches you how to:

- Determine the prerequisites for OS/400 LDAP.
- Configure OS/400 LDAP.
- Start and stop the OS/400 LDAP server.
- Publish OS/400 System Distribution Directories to LDAP.
- Check the connection to OS/400 LDAP.

Task 1: Pre-configuration tasks for OS/400 LDAP

Before configuring OS/400 LDAP, perform the following tasks:

__ 1. Ensure that Directory Services has been installed on the AS/400 or iSeries server. This is included free with OS/400 (option number 32 of 5769-SS1).

Note: In OS/400 V5R1or later, Directory Services is part of the base operating system.

__ 2. Ensure that Operations Navigator is installed and configured. All directory server configuration tasks are performed using Operations Navigator. For more information on Operations Navigator, visit the Web site at:

`http://publib.boulder.ibm.com/pubs/html/as400/v4r5m1/ic2924/index.htm`

__ 3. Ensure you know the password of an OS/400 user profile with *ALLOBJ and *IOSYSCFG special authorities.

__ 4. Define a suffix or naming context for LDAP, if it does not exist yet. This is a Distinguished Name (DN) that defines the name space for your directory. Suggestions for this DN include your organizational unit (ou), organization's name (o) and country (c). For example for this lab we use ou=ITSO,o=IBM,c=US. Defining a suffix to the OS/400 LDAP server does not create a directory entry; a suffix simply identifies to the server that DNs in this namespace can be handled by the OS/400 LDAP server. Other DNs result in a referral to another server or in a “no such object” error.

__ 5. Define an LDAP administrator Distinguished Name (DN) and password, if it does not exist yet. A client authenticated to the server using the LDAP administrator DN and password can create, delete, modify, and read all data in the directory. For this lab we use `cn=Administrator` as the administrator’s DN and `ldappw` as the password.

__ 6. When using V4R5 Operations Navigator or later with V4R5 OS/400 or later, a new user library (QUSRDIRDB) is automatically configured as the LDAP database library. For OS/400 V4R3 and V4R4, you need to identify a library to contain the LDAP database files and specify the name for the local relational database directory entry (typically the AS/400 or iSeries server name).

__ 7. Ensure that TCP/IP is configured correctly on your system. Enter the Change TCP/IP Domain (CHGTCPDMN) command from the command line, press F4, and ensure that the host and domain name is set. Press F3 to exit.

__ 8. Ensure that SMTP information is configured. Enter the Change SMTP Attributes (CHGSMTPA) command from the command line, press F4, and verify the user ID delimiter. You must press Enter because this sets the SMTP default information that may be needed for publishing the mail information to LDAP if the user does not have SMTP information in their system distribution directory entry. Note, in some circumstances, the case of the domain or host name may matter. Therefore, remember whether they are in upper or lower case.

__ 9. Check the system value of QALWUSRDMN “Allow user domain objects in libraries” by entering the Work with System Values (WRKSYSVAL) command. If you changed the QALWUSRDMN system value from *ALL, make sure that it includes QDIRSRV2. Otherwise, can not publish information from the System Distribution Directory (SDD) to the LDAP directory.

Task 2: Configuring OS/400 LDAP

You are now ready to configure the OS/400 LDAP server.

__ 1. Launch Operations Navigator and open the TCP/IP servers folder by selecting **Network->Servers->TCP/IP** node in the Operations Navigator tree (Figure 170).

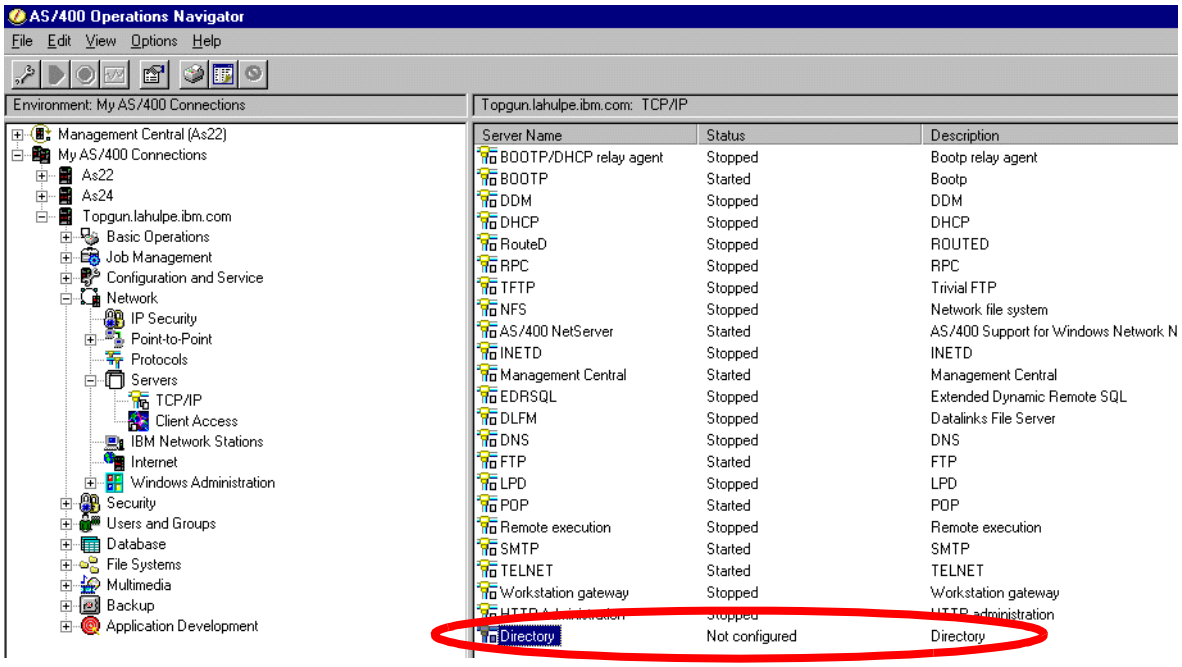

Figure 170. Directory option in Operations Navigator

__ 2. Right-click the **Directory** option that appears in the TCP/IP pane on the right-hand side of the Operations Navigator window. A pop-up context menu appears. Select the **Configure** option.

If you already attempted configuring the Directory Server, you must select the **Re-Configure** pull-down option instead.

__ 3. The Configure Directory Server wizard appears (Figure 171). Click **Next>** to continue.

Note: In OS/400 V5R1 or later, this wizard is different. Here we show the OS/400 V4R5 version.

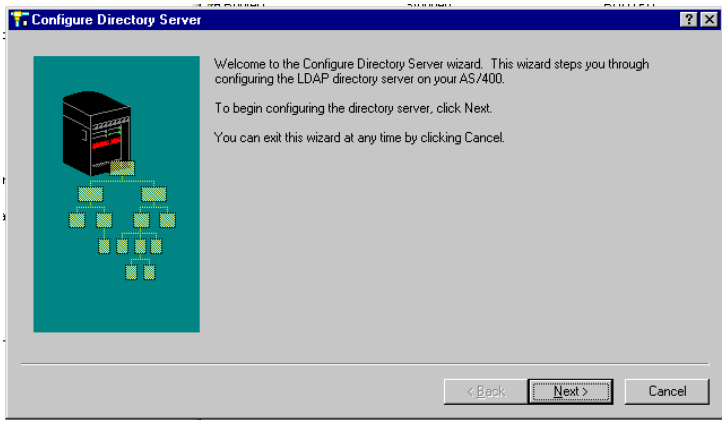

Figure 171. Configure Directory Server wizard

__ 4. On the Administrator Name window, enter the name and password for the LDAP administrator. The default name is cn=Administrator, but this can be changed. However, for this lab, the default value cn=Administrator and a password of `ldappw` have been used (Figure 172). Click **Next>** to continue.

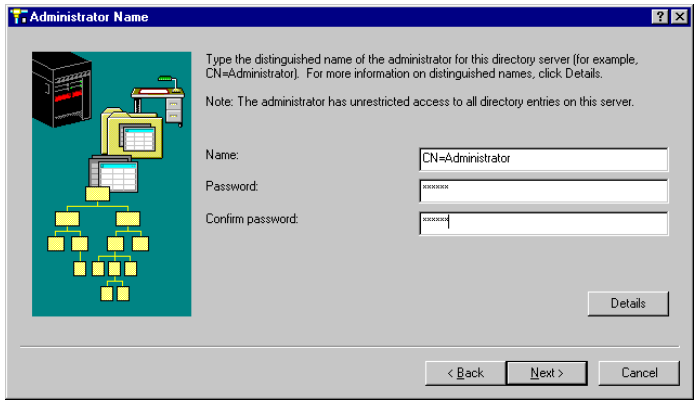

Figure 172. LDAP Administrator name and password

__ 5. On the Choose Directory Suffixes window, the directory suffix must be added to the directory server. Specify the lowest level of the hierarchy first. In this lab, we started at the Organizational Unit (ou) of **ITSO**, then the Organization (o) of **IBM**, and then Country (c) of **US** (Figure 173). Click **Add** and then click **Next>** to continue.

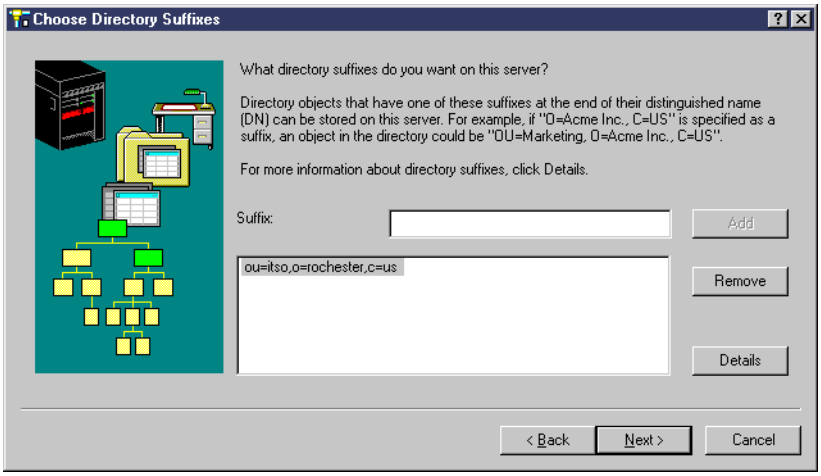

Figure 173. Choose Directory Suffixes

__ 6. On the Start Server when TCP/IP is Started window, the *Yes, start this server when TCP/IP is started* option is already checked (Figure 174). Do not deselect this box. If you do, LDAP does not start when you start TCP/IP on your system. Click **Next>** to finished configuring OS/400 LDAP.

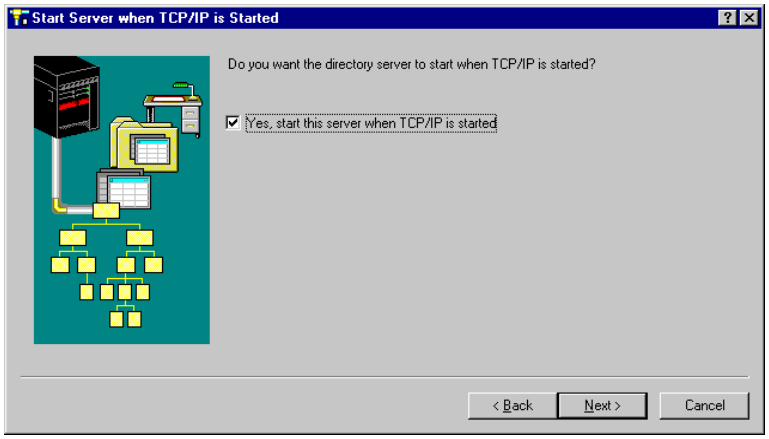

Figure 174. Start LDAP server when TCP/IP is started option

__ 7. On the Configuration Summary window, ensure that the information is correct. Click **Finish** (Figure 175). The Directory server is now configured.

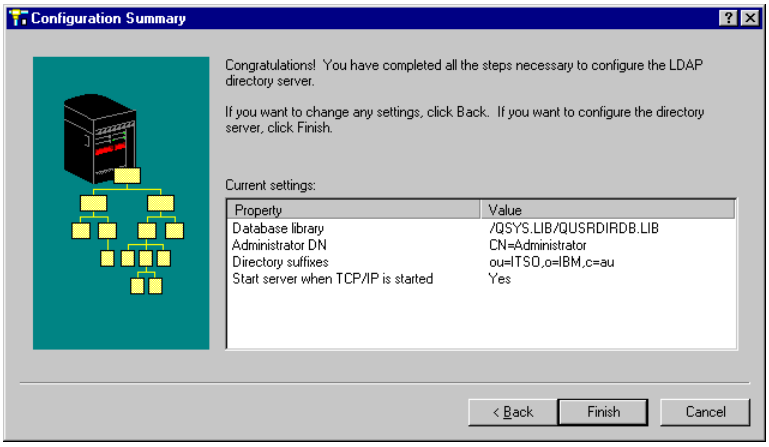

Figure 175. LDAP directory server configuration summary

Task 3: Starting the OS/400 LDAP server

Once LDAP has been configured, you can start the LDAP directory server. From Operations Navigator, right-click the Directory entry in the Network - Servers - TCP/IP panel and select the **Start** option from the pop-up context menu.

You can also start the LDAP directory server from an OS/400 command line by issuing the following Start TCP/IP Server (STRTCPSVR) command:

```
STRTCPSVR *DIRSRV
```

You can see the status of the LDAP directory server in the QDIRSRV job by issuing the following Work with Active Jobs (WRKACTJOB) command:

```
WRKACTJOB SBS(QSYSWRK)
```

Task 4: Publishing to LDAP from the OS/400 System Distribution Directory

After LDAP is configured and running, you can publish users of the OS/400 System Distribution Directory (SDD) to the LDAP directory.

__ 1. From OS/400 Operations Navigator, an initial display of the AS/400 or iSeries server names appears. Right-click the system name from which you want to publish the SDD, and select **Properties** (Figure 176).

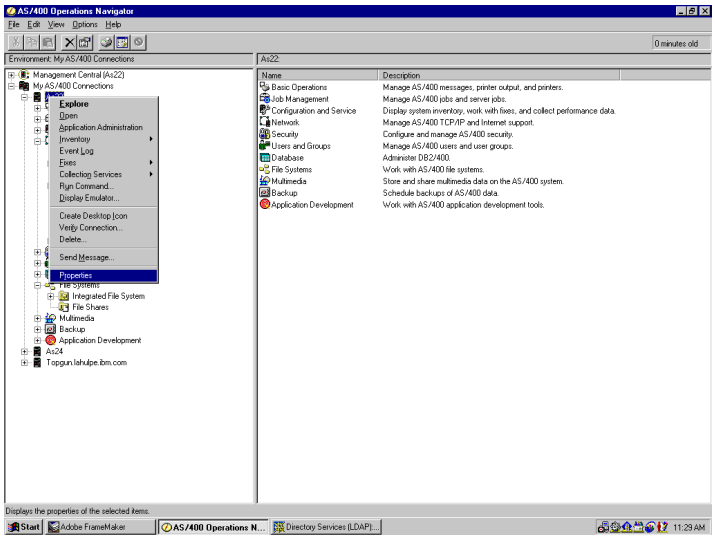

Figure 176. Directory Services properties

__ 2. From the Properties window, click the **Directory Services** tab. Click **Users** from the list that appears to highlight it, and then click the **Configure** button (Figure 177).

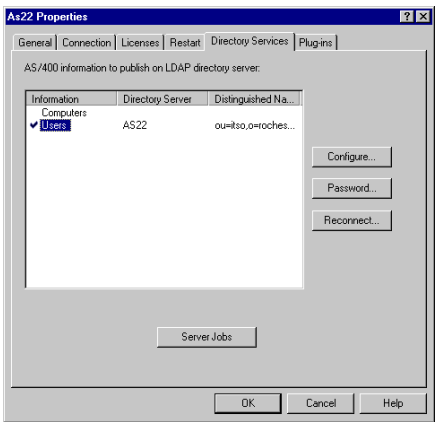

Figure 177. Directory services tab

__ 3. On the Directory Services Publishing - Configure window, select the **Publish AS/400 information for** check box (Figure 178). Enter the following values:

a. In the Where to Publish section, for the “Directory server” parameter, specify the system name that the LDAP server is running on. For this lab, use `PWDI`.

b. For the “Under DN” parameter, enter the DN name you specified when you configured the LDAP server. For this lab, the DN is:

   `ou=ITSO,o=IBM,c=US`

c. In the Server Connection section, specify the “Distinguished Name” parameter of the LDAP server administrator. For this lab, use `cn=Administrator`. This was created when you configured the LDAP server.

d. You also need the administrator Password that you specified when you configured of the LDAP server (`ldappw`).

e. Because you are not setting up SSL in this lab, leave the “Secured Sockets” box un-checked.

f. Leave the port number at the default value 389 since this is the port you configured for the LDAP server.

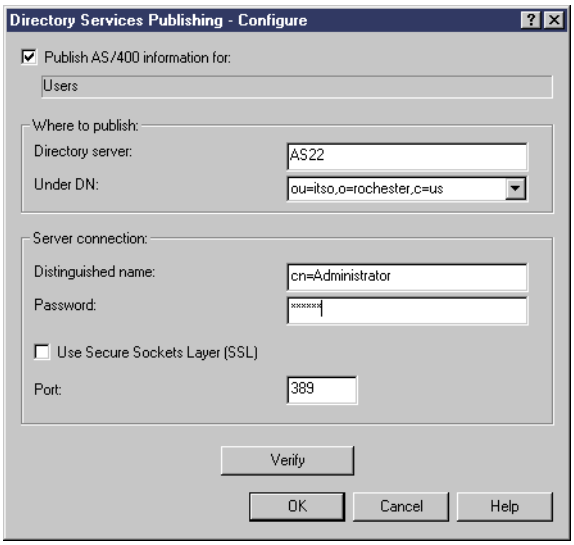

Figure 178. Configuring a connection for publishing SDD

__ 4. Click the **Verify** button to verify that the directory path you specified exists on the LDAP server. This also verifies the Distinguished Name and password to ensure they are valid.

__ 5. If the directory path does not exist, you are prompted to create the path. If you do not create the path, publishing will not be successful. Click **Yes** (Figure 179).

Figure 179. Creating a directory path

__ 6. When the `Directory Services settings verified successfully` message appears, click **OK** (Figure 180).

Figure 180. Verifying settings

__ 7. On the *Directory Service*s window, click **OK** to exit. The SDD is synchronized with the LDAP directory every five minutes under the QGLDPUBA in subsystem QSYSWRK.

__ 8. Click **OK** on the *PWDI Properties* window.

Task 5: Verifying the connection to OS/400 LDAP

This task explains how to check the connection to the OS/400 LDAP directory and verify that the directory entries were published from the OS/400 System Distribution Directory (SDD). There are a number of different methods for doing this. You use the Web browser and, optionally, you can use the Qshell utility.

Note, since the contents of the SDD is published to LDAP only every five minutes, it my take up to

Accessing OS/400 LDAP from a Web browser

Perform the following tasks to access OS/400 LDAP from a Web browser:

__ 1. Check whether you can get a connection to the LDAP server. Open your Netscape browser and type the following location:

```
ldap://PWDI/
```

__ 2. Ensure that your OS/400 user ID has been published from the System Distribution Directory (SDD). Enter the following information in the Netscape browser location:

```
ldap://PWDI/cn=DOMWASxx,ou=ITSO,o=IBM,c=US
```

Accessing OS/400 LDAP from Qshell

Perform the following tasks to access OS/400 LDAP from Qshell:

__ 1. You can also use the Qshell utility to access OS/400 LDAP. To access the Qshell Interpreter, use the OS/400 Start QSH (QSH) command by typing `STRQSH` or `QSH` and press Enter

__ 2. To check that the Administrator password is correct, enter the following information:

```
ldapsearch -v -D cn=Administrator -w ldappw -b cn=monitor -s base
"(objectclass=*)"
```

__ 3. To search and display all directory entries, enter the following information:

```
ldapsearch -v -D cn=Administrator -w ldappw -b ou=ITSO,o=IBM,c=US
"(objectclass=*)"
```